PCT WELTORGANISATION FÜR GE
Internationales I
INTERNATIONALE ANMELDUNG VERÖFFENTL
INTERNATIONALE ZUSAMMENARBEIT AUF DE

WO 9608755A1

(51) Internationale Patentklassifikation 6 : G06F 1/00, 19/00

A1

(11) Internationale Veröffentlichungsnummer: WO 96/08755

(43) Internationales Veröffentlichungsdatum: 21. März 1996 (21.03.96)

(21) Internationales Aktenzeichen: PCT/EP95/03597

(22) Internationales Anmeldedatum: 13. September 1995 (13.09.95)

(30) Prioritätsdaten:
P 44 32 533.9 13. September 1994 (13.09.94) DE
94118018.4 15. November 1994 (15.11.94) EP

(34) Länder für die die regionale oder internationale Anmeldung eingereicht worden ist: AT usw.

(71)(72) Anmelder und Erfinder: ROST, Irmgard [DE/DE]; Niebüller Strasse 19, D-90425 Nürnberg (DE).

(74) Anwälte: TERGAU, Enno usw.; Mögeldorfer Hauptstrasse 51, D-90482 Nürnberg (DE).

(81) Bestimmungsstaaten: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TT, UA, UG, US, UZ, VN, europäisches Patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO Patent (KE, MW, SD, SZ, UG).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: PERSONAL DATA ARCHIVE SYSTEM

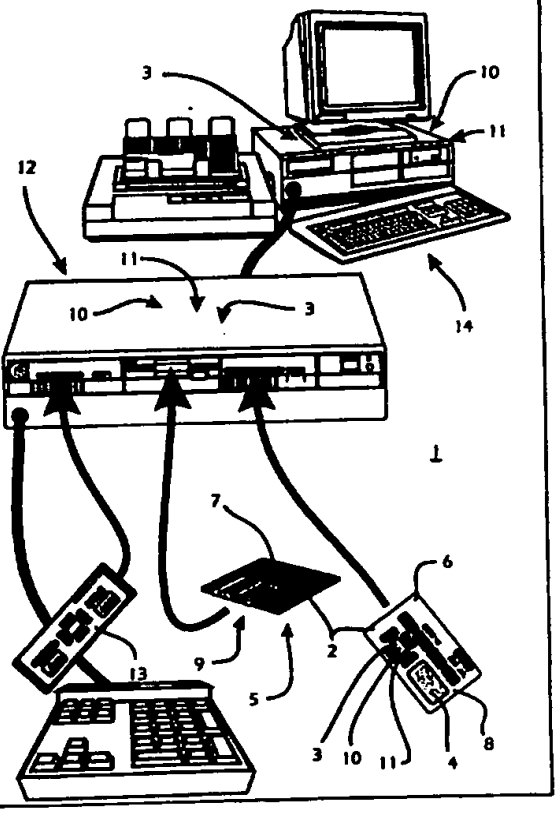
(54) Bezeichnung: PERSONENDATEN-ARCHIVIERUNGSSYSTEM

(57) Abstract

The invention concerns a personal data archive system with portable personal storage devices allowing the owner to enter and store personal data. Authorization checking devices are allocated to the storage devices and grant access to at least some of the personal data stored in the storage devices only in the event of a positive authorization and/or authentication.

(57) Zusammenfassung

Die Erfindung betrifft ein Personendaten-Archivierungssystem mit transportablen, persönlichen Speichereinrichtungen zum Speichern und Aufbewahren von Personendaten beim Inhaber. Dabei sind den Speichereinrichtungen Berechtigungsprüfeinrichtungen zugeordnet, mittels derer nur in Abhängigkeit von einer positiven Berechtigungs- und/oder Authentizitätserkennung ein Zugriff auf zumindest einige der auf den persönlichen Speichereinrichtungen gespeicherten Personendaten freigebbar ist.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AT	Österreich	GA	Gabon	MR	Mauretanien
AU	Australien	GB	Vereinigtes Königreich	MW	Malawi
BB	Barbados	GE	Georgien	NE	Niger
BE	Belgien	GN	Guinea	NL	Niederlande
BF	Burkina Faso	GR	Griechenland	NO	Norwegen
BG	Bulgarien	HU	Ungarn	NZ	Neuseeland
BJ	Benin	IE	Irland	PL	Polen
BR	Brasilien	IT	Italien	PT	Portugal
BY	Belarus	JP	Japan	RO	Rumänien
CA	Kanada	KE	Kenya	RU	Russische Föderation
CF	Zentrale Afrikanische Republik	KG	Kirgisistan	SD	Sudan
CG	Kongo	KP	Demokratische Volksrepublik Korea	SE	Schweden
CH	Schweiz	KR	Republik Korea	SI	Slowenien
CI	Côte d'Ivoire	KZ	Kasachstan	SK	Slowakei
CM	Kamerun	LI	Liechtenstein	SN	Senegal
CN	China	LK	Sri Lanka	TD	Tschad
CS	Tschechoslowakei	LU	Luxemburg	TG	Togo
CZ	Tschechische Republik	LV	Lettland	TJ	Tadschikistan
DE	Deutschland	MC	Monaco	TT	Trinidad und Tobago
DK	Dänemark	MD	Republik Moldau	UA	Ukraine
ES	Spanien	MG	Madagaskar	US	Vereinigte Staaten von Amerika
FI	Finnland	ML	Mali	UZ	Usbekistan
FR	Frankreich	MN	Mongolei	VN	Vietnam

Beschreibung

Personendaten-Archivierungssystem

Die Erfindung betrifft ein Personendaten-Archivierungssystem nach dem Oberbegriff des Anspruchs 1.

In vielen Bereichen des täglichen Lebens werden persönliche Daten benötigt, die häufig jedoch nicht in gesammelter Form zur Verfügung stehen, so daß sie für jeden Bedarfsfall aufwendig zusammengesucht und -gestellt werden müssen. Oft gehen dabei Informationen verloren oder bleiben unberücksichtigt.

Lediglich exemplarisch dafür sind Patientendaten zu nennen, anhand derer nachfolgend einige Probleme bestehender Archivierungssysteme beispielhaft dargestellt werden.

Die medizinischen Daten eines Patienten werden von vielen Einrichtungen des Gesundheitssystems erhoben und dokumentiert. Bei der bislang praktizierten Dokumentation mittels schriftlicher Eintragungen in Krankenblätter, Karteikarten, Ausweise und Pässe (z.B. Diabetiker-Paß) und dem bislang praktizierten Informationsaustausch über die Versendung von Arzt- und Krankenhausentlassungsberichten gehen häufig wichtige medizinische Daten verloren.

Wechselt beispielsweise ein Patient seinen Arzt, so verbleiben die vorher gewonnenen Daten meist in der Kartei des zuletzt behandelnden Arztes und der nächste Arzt beginnt von neuem mit seiner Datensammlung. Hinzu kommt in der modernen Medizin eine zunehmende Aufsplittung der ärztlichen Versorgung in die verschiedenen Fachdisziplinen, wobei oft unter den im Einzelfall beteiligten Kollegen eine ungenügende oder sogar keinerlei Kommunikation erfolgt.

Im derzeit praktizierten Informationssystem werden daher oftmals diagnostische Maßnahmen deswegen wiederholt, weil dem nachbehandelndem Arzt über vorausgegangene Untersuchungen nur schriftlich aufgezeichnete Beurteilungen des Vorgängers vorliegen, nicht aber beispielsweise die ursprünglichen Röntgen- oder Ultraschallbilder oder Labor- und sonstigen Meßprotokolle. Auf Grund im Einzelfall unterschiedlicher Interpretationsmöglichkeiten möchte ein Arzt für seine weiteren Maßnahmen aber verständlicherweise nicht auf eine eigene Beurteilung von Originalunterlagen verzichten.

Ein weiterer gravierender Nachteil des bestehenden Informationsaustausches bei Patientendaten liegt in der Tatsache, daß wichtige medizinische Daten im Notfall oft nicht verfügbar sind. Zwar sind in der Vergangenheit eine Reihe von Pässen und Ausweisen entwickelt worden, wie z.B. der Europäische Notfall-Ausweis, der Impfausweis, der Marcumar-Ausweis, der Allergiepaß u.a., jedoch sind in nachteiliger Weise, sofern den Patienten solche Dokumente überhaupt ausgehändigt wurden, wichtige Daten auf verschiedene Papiere verteilt und Ihr Inhalt ist bei einem Verlust meist nicht rekonstruierbar.

Einen Fortschritt in der Informationstechnologie im Bereich des Gesundheitswesens könnten Patientenkarten in Form von Magnetstreifen- oder Prozessor-Chipkarten darstellen, die in der Lage sind, medizinische Informationen auf einem mobilen elektronischen Datenträger zu speichern. So sind auch in letzter Zeit einige Kartenprojekte entstanden, welche die Nutzung von Prozessor-Chipkarten zur Datenspeicherung im medizinischen Bereich zum Ziel haben.

Die bisher bekannten Entwicklungen von Patientenkarten führen aber nicht zu einer wesentlichen Verbesserung der Datenbasis für die unmittelbare Patientenbetreuung, da auf Grund der begrenzten Speicherkapazität der Prozessor-Chipkarte nur ein kleiner Teil der medizinischen Daten eines Patienten berücksichtigt werden kann. So beinhaltet z.B. die Diabcard (GSF Forschungszentrum für Umwelt und Gesundheit Medis-Institut, Postfach 1129, D - 85758 Oberschleißheim) nur für die Diabetikerbetreuung relevante medizinische Daten. Bei einem anderen Modellprojekt, das von der Kassen-

ärztlichen Vereinigung Koblenz, dem Zentralinstitut für die kassenärztliche Versorgung und der Bundesvereinigung Deutscher Apothekerverbände in den Städten Neuwied und Andernach gestartet wurde ("PraxisComputer", Nr. 4, 15. 06. 94, Seiten 3 bis 6, und Nr. 2, 10. 03. 95, Seiten 8/9), umfaßt der auf einer Patientenkarte gespeicherte Datensatz neben den Anamnesedaten nur noch den Impf- und den Röntgenstatus sowie vom Apotheker an Patienten abgegebene Medikamente.

Ein weiterer bedeutender Nachteil bestehender Speicherkarten besteht darin, daß die gespeicherten Daten nicht wirksam gegen Mißbrauch geschützt sind. Eine reine Verschlüsselung der gespeicherten Informationen ist nicht ausreichend, da mit einem ausreichend großen Aufwand letztendlich jeder Code entschlüsselt werden kann. Im Fall von Patientendaten bedeutet dies, daß letztere, beim Patienten selbst aufbewahrt, leicht auch Unbefugten in die Hände fallen können, die die entsprechenden Informationen nach dem Decodieren der Daten zum Nachteil des Patienten verwenden könnten.

Aus der DE 90 18 059 U1 ist ein System zur Speicherung, Bereitstellung und Aktualisierung von festen und/oder variablen Patienten- und Behandlungsdaten bekannt. Dabei wird von einer stationären Computer-Zentraleinheit mit einer Speichereinheit, in der die in einer Patientenkartei vorhandenen Patientendaten in Form von patientenspezifischen Datensätzen gespeichert sind, und einer Daten-Schnittstelle zur Ein- und Ausgabe von Patientendaten ausgegangen in Verbindung mit einer mobilen Einheit, wie etwa einem portablem Computer, der zur Aufnahme ausgewählter oder aller gespeicherten Patientendatensätze vorgesehen ist. So kann ein Arzt auch bei Hausbesuchen die Informationen seiner elektronischen Patientenkartei nutzen und letztere außer Haus direkt aktuell halten. Ein individueller Patientendatensatz kann über eine Krankenversichertenkarte aufgerufen und aktiviert werden, so daß die verwaltungstechnischen Besuchsdaten direkt erfaßt werden. Wieder zurück in seiner Praxis kann der Arzt dann die Daten auf seiner stationären Computer-Zentraleinheit durch die mobile Einheit aktualisieren.

Der Arzt nimmt hier also seinen eigenen Datensatz zum Patienten mit, anstatt vom Patienten selbst dessen gesammelte Daten von verschiedenen Ärzten und klinischen Einrichtungen zur Verfügung gestellt zu bekommen. Ärztliche Notdienste beispielsweise könnten dieses System bei unbekannten Patienten daher nicht nutzen. Es werden also von Anwendern und nicht von den Personen, welche die Daten betreffen, nur beschränkte Daten lediglich temporär transportabel abgespeichert.

In der DE 38 15 633 C2 ist eine Datenverarbeitungsanordnung zur zentralen Bearbeitung von medizinischen Daten offenbart. Hierbei werden transportable persönliche Speichereinrichtungen verwendet, die für eine vorübergehende Speicherung von laufend erfaßten Biodaten ausgelegt sind. Zumindest in vorgegebenen Zeitabständen werden daher die gespeicherten Daten über eine Telefonstrecke in die Datenverarbeitungsanlage eines Hospitals übermittelt. Sicherheitsaspekte spielen bei diesen Speichereinrichtungen daher keine Rolle.

Die beiden Druckschriften enthalten somit keine über übliche transportable Speichereinrichtungen hinausgehende Lösungen hinsichtlich der dezentralen Archivierung von persönlichen Daten.

Aber auch in anderen Lebensbereichen ist die Zusammenstellung, Handhabung und Verfügbarkeit von persönlichen Daten aufwendig und führt häufig nicht zum angestrebten vollumfänglichen Ergebnis. Neben der oftmals nicht ausreichenden Speicherkapazität der auf Prozessor-Chipkarten verfügbaren Datenspeicher für die gewünschte Datenmenge besteht bei einer Speicherung auf transportablen Massenspeichern die Gefahr einer mißbräuchlichen Verwendung auf Grund einer fehlenden Zugriffsabsicherung.

Es ist somit die Aufgabe der vorliegenden Erfindung, ein Personendaten-Archivierungssystem zu schaffen, das transportable, persönliche Speichereinrichtungen zum Speichern und Aufbewahren von Personendaten beim Inhaber enthält und einen höheren Sicherheitsstandard als aus dem Stand der Technik bekannten Systeme ermöglicht.

Diese Aufgabe wird mit einem Personendaten-Archivierungssystem nach dem Anspruch 1 gelöst.

Durch die Erfindung ist somit bei einem gattungsgemäßen Personendaten-Archivierungssystem vorgesehen, daß den Speichereinrichtungen Berechtigungsprüfeinrichtungen zugeordnet sind, mittels denen nur in Abhängigkeit von einer positiven Berechtigungs- und/oder Authentizitätserkennung ein Zugriff auf zumindest einige der auf den persönlichen Speichereinrichtungen gespeicherten Personendaten freigebbar ist.

Insbesondere sind durch die Erfindung die Sicherheitsnachteile des Standes der Technik behoben. Ein Datenmißbrauch ist zumindest weitgehend unmöglich oder wenigstens in Anbetracht des erforderlichen Aufwandes unrentabel durchzuführen.

Dadurch, daß erfindungsgemäß ein Zugriff zumindest auf einige der Daten nur nach erfolgter Authentisierung und Autorisierung möglich ist, wird sichergestellt, daß die möglicherweise zusätzlich verschlüsselten Daten für Unbefugte nicht zugänglich sind, um diese Daten zur Informationsgewinnung zu decodieren.

Wenn ein solcher berechtigungsabhängiger Zugriff nicht für sämtliche Datenbereiche vorgesehen ist, können auch Daten gespeichert werden, die frei zugänglich sind, wie es beispielsweise für Notfalldaten von Vorteil sein kann.

Als weiterer wesentlicher Vorteil wird durch die Erfindung ferner die Möglichkeit geschaffen, größere persönliche Datenmengen dezentral mit ausreichender Sicherheit zu speichern, wofür transportable Speichereinrichtungen mit größeren Speicherkapazitäten in das System integriert werden können. Solange nämlich nicht die gewünschte Sicherheit der gespeicherten Daten vor unberechtigtem Zugriff realisierbar war, war die entsprechende Speicherung solcher bedeutenden persönlichen Daten im Zuständigkeitsbereich jeder Person selbst aus Datenschutzgesichtspunkten nicht vernünftig durchführbar. Erst durch die vorliegende Erfindung können nun auch große Datenmen-

gen ausreichend geschützt werden, so daß nunmehr überhaupt erst sinnvoll an die Einbindung entsprechend ausreichend großer Speichermedien herangegangen werden kann, wie es beispielsweise durch bevorzugte Ausgestaltungen der Speichereinrichtungen der Erfindung erfolgt ist. D.h., daß es im speichertechnischen Sinn zwar grundsätzlich kein Problem darstellt, Massenspeicher für große Datenmengen bereitzustellen, derartige Speichermedien aber nicht selbst die für die persönlichen Daten erforderliche Zugriffssicherheit bieten, wie sie durch die Erfindung geschaffen wurde.

Beispielsweise kann der Zugang zu den gespeicherten Daten sowie der Umfang dieses Zugangs z.B. außer zu gespeicherten Notfalldaten ausschließlich vom Inhaber der Speichereinrichtungen bestimmt werden.

Die Sicherheitseinrichtungen bei dem erfindungsgemäßen Personendaten-Archivierungssystem, d.h. die Berechtigungsprüfeinrichtungen, können bei einer gegenseitigen Identifizierung von Speichereinrichtungen und Zugriffsgeräten beginnen und über die Registrierung einer Benutzererkennung durch die Berechtigungsprüfeinrichtungen bis zur Nachrichtenverschlüsselung und -authentifikation durch eine z.B. elektronische Unterschrift gehen.

Durch die im Erfindungsumfang enthaltenen Sicherheitsoptionen wird eine äußerst hohe Datensicherheit erreicht, wie sie beispielsweise nicht nur im medizinischen Bereich bislang noch nicht realisiert werden konnte.

Die Erfindung hat außerdem den Vorteil, daß z.B. EDV-Hardware verwendet werden kann, die bereits als Massenprodukt für einen günstigen Preis zur Verfügung steht, was den finanziellen Aufwand vernünftig abschätzen läßt und in vernünftigen niedrigen Grenzen hält. Durch entsprechende Schnittstellen mit gängigen Praxisverwaltungsprogrammen ist die Einbindung der vorgenannten üblichen Hardware oder einer speziellen Hardware und entsprechender Software in die vorhandene Praxis-EDV eines Arztes oder einer klinischen Einrichtung leicht möglich, was in der Bundesrepublik Deutsch-

land z.B. über die vorhandene Schnittstelle "Behandlungsdatenträger" (BDT) gewährleistet ist.

Beispielsweise bei einer Anwendung der Erfindung als Patientendaten-Archivierungssystem kann eine direkte Personalisierung und Aktualisierung relevanter Daten in der Arztpraxis selbst erfolgen. Bereits jetzt ist absehbar, daß medizinische Daten zukünftig immer mehr primär auf z.B. digitalen Medien erfaßt und gespeichert werden. Bei dem erfindungsgemäßen System wird der Patient in die Lage versetzt, sich die Daten noch in der Arztpraxis direkt auf sein Speichermedium überspielen zu lassen, insbesondere medizinische Daten für Ausweisfunktionen und die Auflistung von Diagnosen und Dauermedikationen. Weitere umfangreichere Text- und Bilddaten können alternativ zur Überspielung auf die patientenspezifischen Speichereinrichtungen in der Arztpraxis in Personalisierungsbüros digitalisiert und auf die Speichereinrichtungen geschrieben werden. Eventuell kann vor einer Digitalisierung eine Verkleinerung oder sogar Mikroverfilmung durchgeführt werden, um den Speicherplatzbedarf zu minimieren.

Eine Alternative zu den persönlichen transportablen Speichereinrichtungen könnte in der multimedialen Datenkommunikation ein allgemeiner Datenverbund in der ambulanten Medizin sein, was beispielsweise mit Hilfe der ISDN-Vernetzung realisiert werden könnte. Die Telemedizin wird bereits in Krankenhäusern, Forschungsstätten und an Universitäten erprobt. Bei diesen Projekten geht es in erster Linie um Telekonsultation, also z.B. den Austausch von diagnostischem Bildmaterial zum Zweck der gemeinsamen Befundung. Daneben gibt es in diesem Bereich noch weitere sinnvolle Perspektiven, wie die Telekommunikation im administrativen Sektor oder die Teletherapie.

In der ambulanten Medizin sind aber völlig andere Voraussetzungen und Ziele gegeben. In der ambulanten Medizin kommt der Patient zum Arzt oder umgekehrt. Dabei kann der Patient problemlos als Überbringer von Daten fungieren, wodurch keinerlei Kosten entstehen, wie es im Vergleich mit der Datenvernetzung der Fall wäre. Bei einer Datenaustauschvernetzung besteht weiterhin die Gefahr, Produkte und Dienstleistun-

gen am technisch Machbaren auszurichten und dabei die tatsächlichen Bedürfnisse des Patienten aus den Augen zu verlieren.

Bei der Telemedizin muß mit erheblichen Akzeptanzproblemen gerechnet werden. Der Austausch von persönlichen medizinischen Daten über Datenautobahnen schürt beim Patienten - vielleicht nicht zu Unrecht - die Angst vor dem "gläsernen Patienten". Ferner könnten bei einer Datenfernübertragung unautorisierte Personen eine Möglichkeit haben, an die gespeicherten Daten zu gelangen.

Es liegt aber eine weitere Nutzungsmöglichkeit der vorliegenden Erfindung darin, das Personen- oder insbesondere Patientendaten-Archivierungssystem und die Telemedizin synergetisch zu verbinden. So können die persönlichen Speichereinrichtungen, wie beispielsweise eine Prozessor-Chipkarte in Verbindung mit einem transportablen Massenspeicher unter Einbeziehung von geeigneten Zugriffsgeräten gleichsam als Peripheriestation dienen und patientenbezogene Daten nach erfolgter Schreibzugriffsfreigabe von verschiedenen Quellen aufnehmen. Oder in umgekehrter Richtung kann ein konsiliarisch hinzugezogener Arzt über z.B. das ISDN-Netz auf die Daten der Speichereinrichtungen zugreifen, sobald die Berechtigungserkennung erfolgt ist. Bei einer noch weiteren Anwendung kann ein Patient durch ein persönliches Zugriffsgerät bei einem Anruf bei einem Arzt beispielsweise parallel zum Gespräch über den zweiten Kanal des ISDN-Anschlusses dem Arzt seine Daten von den Speichereinrichtungen zur Verfügung stellen, wobei er mit seiner eigenen Berechtigung für die Zugriffsfreigabe sorgt.

Ein weiterer Vorteil der vorliegenden Erfindung liegt darin, daß bestehende Datensysteme und -strukturen problemlos übernommen und weitergeführt werden können. Z.B. kann bei einem Patientendaten-Archivierungssystem durch die Übernahme vorhandener Protokolle für einen Datenaustausch der in der Bundesrepublik Deutschland bereits eingeführten Krankenkassenkarte und des zugehörigen Lesegeräts ein frei zugänglicher Bereich der Speichereinrichtungen - vorzugsweise eine als eine Art Text- oder Textaufzeichnungskarte fungierende Prozessor-Chipkarte - im Empfangsbereich jeder

Arztpraxis oder in der Aufnahmestation jedes Krankenhauses in Deutschland gelesen werden. Der Zugriff auf die Notfalldaten ist zumindest gegen einen Zugriff durch Ärzte nicht geschützt, so daß diese Daten auch bei Bewustlosigkeit des Patienten zugänglich sind. Alternativ kann als gewisser Schutz der Notfalldaten eine Zugriffsgeräteidentifikation eingebaut sein, wobei Ärzte und Rettungsdienste dann zweckmäßigerweise über geeignete Zugriffsgeräte verfügen. Hierbei bezieht sich die Authentizitätsprüfung bzw. der Authentizitäsnachweis auf z.B. das Lesegerät selbst. Die Prozessorkarte, die ein Beispiel für einen geeigneten Speichereinrichtungsteil ist, ermittelt in diesem Fall also bedienerunabhängig, ob das jeweilige Lesegerät zugriffsberechtigt ist. Diese so gearte-
10 te Prüfung kann auch für andere Datenbereiche als den Notfalldatenbereich verwendet werden.

Eine andere Möglichkeit, die Daten, die die Versorgung für den medizinischen Notfall betreffen in in einer Notsituation nicht hinderlicher Weise zu schützen, so daß sie nur
15 einem bestimmten Personenkreis ohne großen Aufwand zugänglich sind, besteht in einer Arztkarte, durch die eine entsprechende Zugriffsfreigabe erreicht wird. Mit der Arztkarte oder allgemein einer "Profikarte" oder Berechtigungskarte kann sich eine per se zugriffsberechtigte Person gewissermaßen z.B. in ein Lesegerät einloggen. Bis zum Ausloggen der Person können über das Lesegerät die soweit freigegebenen Daten auf
20 den Speichereinrichtungen gelesen werden. Somit kann personenbezogen die Zugriffsberechtigung medizinischer Leistungsbringer geregelt werden.

In jedem Fall (auch dem vorher geschilderten) wird auf der beispielsweise als ein Teil der Speichereinrichtungen vorgesehenen Prozessorkarte nach einem Zugriff vermerkt,
25 mit welchen Lesegerät bzw. mit welcher Profikarte auf die Prozessorkarte zugegriffen wurde. So kann z.B. das Lesegerät eines bestimmten Krankenwagens ermittelt werden, über das ein Zugriff ausgeführt wurde. Über den Dienstplan kann dann der Name des verantwortlichen Arztes ermittelt werden. Verläuft eine Authentizitätsprüfung positiv, so erfolgt auch gleichzeitig die Autorisierung für einen Speicherzugriff durch z.B. die Pro-
30 zessorkarte selbst.

Nur die sonstigen Daten z.B. der Textkarte und einer Bild- oder Bildaufzeichnungskarte als Massenspeicher, die durch einen Massenspeicher gebildet ist, können beispielsweise erst nach Eingabe einer nur dem Patienten bekannten, persönlichen Identifikationsnummer (PIN) abgerufen werden. Die Eingabe der PIN erfolgt durch den Patienten über eine separate Zahlentastatur im Sprechzimmer des Arztes. Auf z.B. der Prozessorkarte als einerseits Berechtigungseinrichtungsbestandteil und andererseits Speichereinrichtungsteil ist gewissermaßen ein Inhaltsverzeichnis der gesamten Speichereinrichtungen hinterlegt.

Aktuelle Untersuchungsbefunde, wie Labor- oder Blutdruckwerte, Daten für Vor- und Nachsorgeuntersuchungen, Pässe usw. können jederzeit vom behandelnden Arzt direkt in der Sprechstunde zur laufenden Dokumentation ergänzt werden. Ferner können z.B. Krankenkassen Updates versenden, die mittels eigenen Geräten, beim Arzt oder bei der Krankenkasse installiert werden können. Diese Daten können auf einem Massenspeicher beispielsweise in verschlüsselter Form vorliegen. Nur durch einen chipkarten-gestützten oder -freigegebenen Zugriff sind bei einem Ausführungsbeispiel diese Daten entschlüsselbar, wofür wegen der eventuell sehr großen Datenmenge ein Coprozessor als Kryptoeinheit eingesetzt wird, die z.B. ebenfalls auf der Chipkarte angeordnet ist.

Gemäß einer vorteilhaften Weiterbildung der Erfindung kann mittels den Berechtigungsprüfeinrichtungen eine Mehrzahl von Prüfstufen ausführbar sein. Der damit erzielbare Vorteil liegt darin, daß die gespeicherten Daten abgestuft vor unberechtigten Zugriffen geschützt werden können. So kann es beispielsweise wünschenswert sein, daß zumindest im eigenen Beisein ein Apotheker auf Informationen betreffend bisher verabreichte Medikamente zugreifen kann, ein Sachbearbeiter einer Bank bei einem Bankwechsel Dauerauftrags- und Einzugsermächtigungsdaten in die Datenbank des neuen Instituts überführt, ein Taxifahrer sich die exakt bezeichnete Zieladresse auf seinem Display anzeigen lassen kann, um nicht durch einen Verständigungsfehler zu einem falschen Ziel zu fahren oder das Ziel nicht zu kennen, usw.

Bei einer bevorzugten Ausgestaltung der Erfindung enthalten die Speichereinrichtungen zumindest teilweise ein zum Hinzufügen und/oder Ändern von Personendaten beschreibbares und insbesondere wiederbeschreibbares Speichermedium. Damit können in vorteilhafter Weise die gespeicherten Informationen problemlos aktuell gehalten werden, ohne bei Datenänderungen oder -hinzufügungen immer wieder neue komplette Speichereinrichtungen herstellen zu müssen, was im Hinblick auf eine möglichst große Sicherheit in Abhängigkeit von konkreten Anwendungsfällen aber auch Vorteile hat. Ein wiederbeschreibbares Speichermedium hat den Vorteil, daß der vorhandene Speicherplatz optimal genutzt werden kann, da keine unnötigen oder veralteten Daten gespeichert bleiben. Ein einmalig beschreibbares Speichermedium hat den Vorteil, daß Daten nicht versehentlich gelöscht werden und dabei unwiederbringbar verloren gehen können.

Dadurch, daß die Berechtigungsprüfeinrichtungen zum Freigeben eines Lese- und/oder Schreibzugriffs auf das beschreibbare Speichermedium in Abhängigkeit von einer insbesondere entsprechenden Berechtigungs- und/oder Authentizitätserkennung ggf. in einer zugehörigen Prüfstufe ausgelegt sind, kann vorteilhaft sichergestellt werden, daß die Zugriffsberechtigung möglichst praxisgerecht handhabbar ist. Dasselbe trifft für den Fall zu, daß zumindest ein Teil des beschreibbaren Speichermediums schreibgeschützt oder schreibschützbar ist, wie bei einer Weiterbildung der Erfindung vorgesehen ist.

Wenn die Speichereinrichtungen einen ersten Teil und zumindest einen zweiten Teil mit insbesondere unterschiedlichen Speicherkapazitäten enthalten, wird eine Grobeinteilung der zu speichernden oder gespeicherten Daten möglich, wobei z.B. ein kleiner, schneller Speicher für häufig genutzte Daten und ein großer, langsamer Speicher für selten benötigte große Datenmengen mit Vorteil einsetzbar ist. Ferner kann ein Speicher für die Entscheidungsfindung der Berechtigungsprüfeinrichtungen erforderliche Informationen enthalten, wodurch auch der andere Speicher geschützt wird.

Bei einer bevorzugten Ausführungsform der Erfindung ist der erste Teil der Speichereinrichtungen kapazitätsmäßig am kleinsten und ein Ausweis-, Identifikations- oder

Stammdatenspeicherteil. Praktischerweise kann gemäß einer Weiterbildung dieser Ausführung auf die auf dem ersten Teil der persönlichen Speichereinrichtungen gespeicherten Personendaten, wie Ausweis-, Identifikations- oder Stammdaten, unabhängig von den Berechtigungsprüfeinrichtungen oder mit einer positiven Berechtigungs- und/oder Authentizitätserkennung in einer ersten Prüfstufe der Berechtigungsprüfeinrichtungen zugegriffen werden. Damit steht ein Speicher zur Verfügung, der z.B. zum Speichern von Notfalldaten geeignet ist, die auch ohne Mitwirkung des Inhabers zugänglich sein sollten.

Eine besonders bevorzugte Ausführungsform der Erfindung ist dergestalt, daß nur in Verbindung mit wenigstens dem ersten Teil der Speichereinrichtungen auf zumindest einen zweiten Teil der Speichereinrichtungen zugegriffen werden kann. Dies ist eine besonders sichere Struktur, um einen unbefugten Zugriff auf die Informationen im zweiten Teil der Speichereinrichtungen auszuschließen.

In weiterer Ausgestaltung beispielsweise der vorstehenden Ausführungsform ist erfindungsgemäß bevorzugt, daß der zweite, relativ zum ersten Teil kapazitätsmäßig größere Teil der Speichereinrichtungen ein Detaildatenspeicherteil ist, dessen Inhalt somit besonders sicher ist. Diese Sicherheit kann weiter dadurch erhöht werden, daß auf die auf dem zweiten Teil der persönlichen Speichereinrichtungen gespeicherten Personendaten, wie Detaildaten, nur in Abhängigkeit von einer positiven Berechtigungs- und/oder Authentizitätserkennung ggf. in einer zweiten Prüfstufe mittels der Berechtigungsprüfeinrichtungen zugreifbar ist.

Eine weitere besonders bevorzugte Realisierung der Erfindung besteht darin, daß die wenigstens ersten und zweiten Teile der Speichereinrichtungen durch separate erste bzw. zweite Speichervorrichtungen insbesondere auf verschiedenen ersten bzw. zweiten Datenträgern gebildet sind. Die räumliche Trennung der Speichereinrichtungsteile insbesondere auf separaten Datenträgern trägt in vorteilhafter und besonders einfacher Weise zu einer hohen Sicherheit des erfindungsgemäßen Systems bei, da es dadurch möglich ist, den Datenträger mit den kritischeren Daten sicher aufzubewahren, solange

er nicht benötigt wird, was meist relativ selten der Fall ist. Ferner kann das System so eingerichtet sein, wie weiter oben angegeben ist, daß auf den zweiten Speichereinrichtungsteil nur in Kombination mit dem ersten Speichereinrichtungsteil zugegriffen werden kann. Wird somit dafür gesorgt, daß nicht beide Speichereinrichtungsteile gemeinsam abhanden kommen können, sind die Daten auf dem zweiten Speichereinrichtungsteil absolut sicher.

Gemäß bevorzugten Ausführungen der Erfindung ist der erste Teil der Speichereinrichtungen bzw. die erste Speichervorrichtung eine magnetische, magneto-optische oder optische Speicherfläche oder ein Speicherchip insbesondere auf oder in einer vorzugsweise etwa scheckkartengroßen Kunststoffkarte als Datenträger. Ferner ist der zweite Teil der Speichereinrichtungen bzw. die zweite Speichervorrichtung bevorzugt ein elektronischer, magnetischer (z.B. Diskette oder Streamer-Tape), magneto-optischer oder optischer (z.B. CD-ROM ggf. beschreibbar oder WORM: "Write Once Read Many") Massenspeicher insbesondere in Form einer 2,5 oder 3,5 Zoll großen Diskette oder ein Halbleiterspeicher einer PCMCIA-Einheit (Personal Computer Memory Card International Association) als Datenträger. Als eine derartige Kombination können beispielsweise eine Prozessor-Chipkarte mit den Berechtigungsprüfeinrichtungen und einem kleineren Speicher und eine MO- (magneto-optische) Platte zur Speicherung großer Datenmengen einschließlich Bildern kombiniert eingesetzt werden, wobei der Zugriffsschutz der MO-Platte durch die Prozessor-Chipkarte erfolgt, für einen Zugriff auf die MO-Platte also zumindest die Prozessor-Chipkarte vorhanden sein muß.

Die Verteilung z.B. medizinischer Informationen auf beispielsweise eine Prozessor-Chipkarte und ein Massenspeichermedium gewährleistet einen per se abgestuften Datenzugang und somit eine hohe Sicherheit, die weiterhin dadurch erhöht wird, daß die Chipkarte gewissermaßen als Schlüssel einerseits für einen Zugriff auf die auf ihr selbst gespeicherten Daten und andererseits auf das Massenspeichermedium fungiert. Zusätzlich können auch noch die Daten auf dem Massenspeichermedium verschlüsselt sein, um eine noch höhere Sicherheit zu gewährleisten.

Als Prozessor-Chipkarte, die bei der vorstehend beschriebenen Kombination mit einem Massenspeicher als "Textkarte" fungiert, kann eine Prozessorkarte entsprechend den geltenden DIN-Vorschriften oder ISO-Standards mit einer Speicherkapazität von acht oder sechszehn Kilobytes verwendet werden, was bei einer Komprimierung der darauf zu speichernden Daten eine ausreichende Informationsmenge für Notfälle und Übersichten ermöglicht. Der Massenspeicher, der auch als "Bildspeicher" bezeichnet werden kann, hat als Minidisk oder magneto-opische Platte (MO-Platte) beispielsweise eine Kapazität von 140 Megabyte oder sogar bis zu 650 Megabyte. MO-Platten sind mit 2,3 oder 3,5 Zoll relativ klein und handlich und können ausreichend große Datenmengen aufnehmen. Hinzu kommt, daß die Daten auf einer MO-Platte beliebig oft überschrieben, aber unter Alltagsbedingungen nicht versehentlich gelöscht werden können.

Die Textkarte speichert in Schriftform vorliegende Informationen und leistet durch eigene "Intelligenz" den Zugriffsschutz für beide Datenträger beispielsweise unter Einbeziehung von Verschlüsselungsalgorithmen, während die Bildkarte die Speicherung von großen Datenmengen übernimmt, also von Abbildungen (Röntgen-, Ultraschall- und Endoskopiebilder usw.), von Biosignalen (z.B. EKG, EEG) oder auch von Texten zur Anamnese, die auf der Prozessorkarte keinen Platz mehr finden. Insbesondere kann die Textkarte bei einem Patientendaten-Archivierungssystem Informationen, wie Verwaltungsdaten, einen Notfall-Ausweis, Anamnese, Befund, Vor- und Nachsorge sowie einen Paß u.ä. enthalten.

Für die Erfindung kommt es jedoch nicht darauf an, ob und ggf. wie die Speichermedien zusammengesetzt sind, sondern nur darauf, daß ein wirksamer Zugriffsschutz realisiert ist. Beispielsweise kann ein optischer Speicher mit sehr großer Kapazität auch als einziger Speicher verwendet und auf einer etwa scheckkartengroßen Kunststoffkarte untergebracht werden. Durch physikalisches Lochbrennen sind beispielsweise Speicherkapazitäten im Bereich von 1 Gigabyte pro cm^2 Kunststoffolie als Datenträger möglich, so daß bezüglich einer so ausgestalteten Karte externe Massenspeicher unnötig sind.

Ein vorzugsweiser Aufbau der Erfindung besteht darin, daß zumindest einem Teil der Speichereinrichtungen Prozessoreinrichtungen zugeordnet sind, die vorzugsweise auf dem Datenträger, wie z.B. einer Kunststoffkarte, angeordnet sind und insbesondere einen Prozessor enthalten. Besonders vorteilhaft können derartige Prozessoreinrichtungen für die Berechtigungsprüfeinrichtungen genutzt werden. Die Prozessoreinrichtungen gewährleisten dabei durch eine eigene "Intelligenz" den Zugriffsschutz für die Speichereinrichtungen. Dabei ist weiterhin bevorzugt, daß die Prozessoreinrichtungen zur Steuerung von zumindest Teilen der Speichereinrichtungen und/oder zur wenigstens teilweisen Steuerung von Zugriffen auf letztere und/oder insbesondere als Teil der Berechtigungsprüfeinrichtungen ausgelegt sind.

Zur Erhöhung der Datensicherheit ist es ferner von Vorteil, wenn den Speichereinrichtungen Kryptoeinrichtungen vorgeschaltet sind, deren Betrieb insbesondere mittels der Berechtigungsprüfeinrichtungen zur Bearbeitung von Zugriffen auf die Speichereinrichtungen freigebbar ist. D.h., daß ein Ver- und Entschlüsseln der gespeicherten Daten von einer Zugriffsfreigabe durch die Berechtigungseinrichtungen abhängt. Bevorzugt sind die Kryptoeinrichtungen in ggf. vorhandenen Prozessoreinrichtungen enthalten und weisen vorzugsweise einen Kryptoprozessor auf.

Wenn ein Teil der Speichereinrichtungen und/oder die Berechtigungsprüfeinrichtungen auf einer Prozessor-Chipkarte realisiert sind, kann beispielsweise letztere auch eine Kryptoeinheit aufnehmen. Prozessoreinrichtungen können aber auch ganz oder teilweise in einem Zugriffsgerät oder in zugeordneten Rechnereinrichtungen untergebracht sein.

Allgemein können Kryptoeinrichtungen z.B. ein asymmetrisches Verschlüsselungsverfahren (RSA) verwenden.

Um zu verhindern, daß unerwünschte Kopien der gespeicherten Daten angefertigt werden können, sieht eine Fortbildung der Erfindung vor, daß Kopierschutzeinrichtungen vorgesehen sind, mittels denen ein Speichern von zumindest einigen Daten, die auf

den persönlichen Speichereinrichtungen, insbesondere ggf. deren zweiten Teil, gespeichert sind, auf bezüglich letzteren externen Speichern unterbindbar ist und/oder ein Speichern von zumindest einigen Daten, die auf dem ersten Teil der Speichereinrichtungen gespeichert sind, auf bezüglich letzteren externen Speichern zulaßbar sind. Letzteres ermöglicht z.B. die problemlose Übernahme von Patientenname, -adresse und Krankenkassendaten für die Rezeptausstellung und Behandlungsabrechnung.

In ähnlicher Weise wirken Druckausgabeschutzeinrichtungen, die vorgesehen sein können und mittels denen eine Druckausgabe von zumindest einigen Daten unterbindbar ist, die auf den persönlichen Speichereinrichtungen, insbesondere ggf. deren zweiten Teil, gespeichert sind und/oder ein Drucken von zumindest einigen Daten zulaßbar ist, die auf dem ersten Teil der Speichereinrichtungen gespeichert sind. Letzteres ermöglicht eine problemlose Erstellung z.B. eines schriftlichen Behandlungsberichts für einen Arzt.

Um zu verhindern, daß die einer Person genehmigte Einsichtnahme in die Daten durch Harware-Einrichtungen gleichzeitig unbeabsichtigt beispielsweise über zusätzliche Bildschirme oder mittels Netzwerkkarten sogar andere Rechner auch weiteren Personen zugänglich sind, sollten Ausgabebeschränkungseinrichtungen vorgesehen sein, mittels denen eine Ausgabe von zumindest einigen Daten, die auf den persönlichen Speichereinrichtungen, insbesondere ggf. deren zweiten Teil, gespeichert sind, auf mehr als ein Ausgabemedium unterbindbar ist.

Um jedoch willentliche Kopien, Druckausgaben und Mehrbildschirmanzeigen, Netzwerkübertragungen etc. der aufgerufenen Daten zuzulassen, können die entsprechenden vorgenannten Schutzeinrichtungen mittels der Berechtigungsprüfeinrichtungen durch eine entsprechende positive Berechtigungs- und/oder Authentizitätserkennung ggf. in einer zugehörigen Prüfstufe neutralisiert werden.

Eine einfache, schnelle und wirkungsvolle Sicherungseinrichtung besteht darin, daß die Berechtigungsprüfeinrichtungen ausgelegt sind, Gerätekennungen von Zugriffsgeräten

für die Handhabung der Speichereinrichtungen in eine Prüfung zur Berechtigungs- und/oder Authentizitätserkennung ggf. zur Erfüllung einer insbesondere ersten Prüfstufe einzubeziehen. Eine derartige Berechtigungsprüfung kann z.B. für eine Zugriffsfreigabe auf Notfalldaten ausreichend sein und durch Bereitstellen entsprechender Zugriffsgeräte für Notdienstpersonal oder -fahrzeuge sicher realisiert werden.

Zusätzlich oder alternativ können die persönlichen Speichereinrichtungen Kennungen aufweisen, die von den Berechtigungsprüfeinrichtungen in eine Prüfung zur Berechtigungs- und/oder Authentizitätserkennung ggf. zur Erfüllung einer insbesondere ersten Prüfstufe einbeziehbar sind. Damit kann beispielsweise sichergestellt werden, daß es sich nicht um gefälschte Speichereinrichtungen handelt, deren falsche Daten im medizinischen Bereich zu einer gefährlichen Falschbehandlung führen können. Auch daran ist deutlich zu sehen, wie wichtig z.B. im Bereich der Patientendatenarchivierung die zuverlässige Bereitstellung der richtigen Daten ist.

Die bei der vorliegenden Erfindung bevorzugt eingesetzten Sicherheitskomponenten sind Benutzer- und/oder Inhaberidentifikationen von zumindest einem Anwender bzw. dem Inhaber, dessen Daten in den Speichereinrichtungen archiviert sind. Derartige Kennungen werden von den Berechtigungsprüfeinrichtungen vorzugsweise in eine Prüfung zur Berechtigungs- und/oder Authentizitätserkennung ggf. zur Erfüllung einer insbesondere zweiten Prüfstufe und ggf. weiterer Prüfstufen zur Freigabe eines Zugriffs auf zumindest einige der auf den persönlichen Speichereinrichtungen gespeicherten Personendaten einbezogen.

Besonders einfache Möglichkeiten zur Eingabe von Anwenderkennungen, wie eine Benutzer- bzw. Inhaberidentifikation, für die Berechtigungsprüfeinrichtungen erfolgt über manuelle und/oder elektronische Eingaben, wie beispielsweise von einer Berechtigungskarte.

Um jederzeit vorgenommene Informationszugriffe und Einträge personell zuordnen zu können, ist es vorteilhaft, wenn durch die Berechtigungsprüfeinrichtungen zugelassene

Zugriffe auf den Speichereinrichtungen mit den dafür relevanten Daten, wie Gerätekennungen von Zugriffsgeräten und/oder Benutzer- und/oder Inhaberidentifikationen, insbesondere auf den Speichereinrichtungen selbst dokumentierbar sind.

Um dem Inhaber der Speichereinrichtungen die darin oder darauf enthaltenen Informationen zugänglich zu machen, oder um ihm selbst Aktualisierungen zumindest bestimmter Daten zu ermöglichen, sind bei einer vorzugsweisen Ausgestaltung des erfindungsgemäßen Systems persönliche Zugriffsgeräte vorgesehen, mittels denen vom Inhaber, dessen Daten in den Speichereinrichtungen archiviert sind, und/oder von Anwendern der Speichereinrichtungen in Abhängigkeit von einer insbesondere entsprechenden Berechtigungs- und/oder Authentizitätserkennung ggf. in einer zugehörigen Prüfstufe auf zumindest einige der archivierten Daten zum Zweck der Information, Datenänderung/-ergänzung und/oder Weitergabe auch über Datenfernübertragung zugreifbar ist. Damit können z.B. auch bei telefonischen Beratungen, Vereinbarungen, Bestellungen etc. erforderliche Daten problemlos dem Gesprächspartner zur Verfügung gestellt werden. Eine derartige Datenfernübertragung wird z.B. durch das zweikanalige ISDN-Netz begünstigt, in dem ohne weiteres die Gesprächs- und die Datenübertragung gleichzeitig möglich sind.

Für Kunden-, Patienten- und Mandantenbesuche einerseits und die Arbeit in der Firma, Praxis bzw. Kanzlei andererseits ist es weiter von Vorteil, wenn mobile und/oder stationäre Zugriffsgeräte vorgesehen sind, mittels denen von Anwendern in Abhängigkeit von einer insbesondere entsprechenden Berechtigungs- und/oder Authentizitätserkennung ggf. in einer zugehörigen Prüfstufe auf zumindest einige der archivierten Daten zum Zweck der Information und/oder Datenänderung/-ergänzung zugreifbar ist. Dadurch kann das System überall und jederzeit einsatzbereit gehalten und können z.B. auch Rettungsfahrzeuge, Polizeifahrzeuge usw. problemlos so ausgestattet werden, daß eine Nutzung der gespeicherten Informationen an jeglichem Einsatzort möglich ist.

Für die Kosten der Zugriffsgeräte ist es von Vorteil, daß letztere beispielsweise grundsätzlich für einen Schreib- und/oder Lesezugriff ausgelegt sind, wobei zumindest auf

einige der auf den persönlichen Speichereinrichtungen gespeicherten Personendaten eben in Abhängigkeit von einer insbesondere entsprechenden Berechtigungs- und/oder Authentizitätserkennung ggf. in einer zugehörigen Prüfstufe zum Schreiben und/oder Lesen zugegriffen werden kann.

Für die bereits weiter oben angegebene besonders einfache Berechtigungsüberprüfung ist vorgesehen, daß die Zugriffsgeräte Gerätekennungen aufweisen, die von den Berechtigungsprüfeinrichtungen zur Prüfung einer Berechtigungs- und/oder Authentizitätserkennung ggf. zur Erfüllung einer insbesondere ersten Prüfstufe erfaßbar sind, und daß die Gerätekennung vorzugsweise durch eine in zumindest ein Zugriffsgerät eingebbare Anwenderkennung aktivierbar ist.

Das System kann besonders kostengünstig und einfach aufgebaut werden, wenn zum Ansteuern der Zugriffsgeräte herkömmliche Rechnereinrichtungen, wie PCs, vorgesehen sind. Weiterhin wird ein günstiger Aufbau des erfindungsgemäßen Personendaten-Archivierungssystems dadurch gefördert, daß die Zugriffsgeräte entsprechend den Formaten von die Speichereinrichtungen aufnehmenden Datenträgern Kartenlesegeräte für z.B. Magnetstreifen- oder Chipkarten, Diskettenlaufwerke für z.B. magnetische, magneto-optische oder optische Disketten, CD-ROM-Laufwerke und/oder Aufnahmen für PCMCIA-Einheiten enthalten, wie sie insbesondere weitverbreitet angeboten werden. Ein Sicherheitsrisiko entsteht dadurch nicht, da die Datensicherheit durch die Berechtigungsprüfeinrichtungen gewährleistet wird. Ferner können herkömmliche Rechnereinrichtungen, einschließlich wenigstens Bildschirm, Tastatur und Drucker, kostengünstig als Anzeige- und Ein-/Ausgabegeräte von Daten vorgesehen werden.

Eine besonders effiziente, sichere und zuverlässige Ausgestaltung der Zugriffsgeräte sowie ein entsprechender Betrieb des Systems nach der Erfindung besteht darin, daß zumindest zwei Zugriffsgeräte zur Zusammenschaltung von entsprechenden Datenträgern der Speichereinrichtungen insbesondere zu einem Gesamtgerät kombiniert sind und diese Zusammenschaltung von den Berechtigungsprüfeinrichtungen zum Berechtigungsnachweis oder ggf. als eine erste Prüfstufe erfaßbar ist. Beispielsweise kann ein

kombiniertes Zugriffsgerät für eine Prozessor-Chipkarte und einen Massenspeicher als Bestandteile der Speichereinrichtungen vorgesehen werden. Die Berechtigungsprüfeinrichtungen können hierbei besonders einfach realisiert werden, da die Schaltung fest vorgegeben sein kann. Insbesondere können die Sicherheitseinrichtungen in Form der Berechtigungsprüfeinrichtungen unabhängig vom Betriebssystem eines zur Steuerung, Bedienung und Auswertung verwendeten Rechners betrieben werden. Vor allem bei dieser Ausführungsform, aber grundsätzlich auch jeder anderen geeigneten Gestaltung der Erfindung, kann besonders einfach und effizient eine Zugriffsgerätekennung zum Datenschutz eingesetzt werden.

Zunächst kann dabei eine Autorisierung des Benutzers erfolgen. Es wird nur dann ein Zugriff auf das Speichermedium erlaubt, wenn das verwendete Zugriffsgerät, das ein geeignetes Laufwerk sein kann, insbesondere für zwei Datenträger, wie z.B. eine Prozessor-Chipkarte und eine Minidisk, mit einer Kennung ausgestattet ist. Dadurch wird gewährleistet, daß nur entsprechend ausgerüstete Zugriffsgeräte, die auch nur für einzelne Datenträger ausgelegt sein können, für Schreib- und/oder Leseoperationen benutzt werden können, was sicherstellt, daß nur dafür autorisierte Einrichtungen Zugang zu den Daten der Speichereinrichtungen erhalten.

Bei einem Ausführungsbeispiel der Erfindung haben zur Datensicherung sowohl das Lesegerät einer Prozessor-Chipkarte als auch das Laufwerk einer Diskette je eine Kennung. Dabei ist die Diskette nur lesbar, wenn die Lesegerätekennung die Prozessorkarte autorisiert und gleichzeitig die Laufwerkskennung die Diskette autorisiert und gleichzeitig die Prozessorkarte die Diskette freigibt.

Ferner kann bereits über die Zugriffsgerätekennung jeglicher Zugriff auf die Daten der Speichereinrichtungen dokumentiert werden. Dies würde in der Weise erfolgen, daß bei Verwendung des Zugriffsgeräts, wie eines einzelnen oder für mehrere Speichervorrichtungen kombinierten Laufwerks, die entsprechende Kennung als Stempel an einem dafür vorgesehenen Speicherplatz z.B. auf der Prozessor-Chipkarte als Teil der Speichereinrichtungen hinterlassen wird.

Schließlich ist über die aufgezeichnete Zugriffsgerätekennung eine Identifikation des Benutzers möglich. Damit kann nachgewiesen werden, in welcher Arztpraxis oder in welchem Rettungswagen auf die Daten der Speichereinrichtungen zugegriffen wurde. Durch entsprechende Maßnahmen, wie z.B. turnusmäßiger Wechsel der Kennung, kann damit auch für die Authentifikation des Benutzers gesorgt werden.

Damit ein sicherheitstechnisch zwar nicht zu fürchtender, informationstechnisch jedoch äußerst unangenehmer Datenträgerverlust sich nicht negativ auf die Datenarchivierung auswirkt, sollten von allen Datenträgern Sicherungskopien erstellt und aufbewahrt werden. Bevorzugt sind die Zugriffsgeräte ausgelegt, ohne Berechtigungsnachweis oder ggf. in einer ersten Prüfstufe Sicherungskopien der transportablen, persönlichen Speichereinrichtungen zu erstellen. Besondere Sicherheitsmaßnahmen sind dabei deshalb nicht zu beachten, da für den Zugriff auf Kopien der Speichereinrichtungen dieselben Maßgaben gelten, wie für die Originale.

Für einen bevorzugten Einsatz des erfindungsgemäßen Personendaten-Archivierungssystem sind gewisse Anpassungen an die Handhabung von Patientendaten vorteilhaft, wie z.B., daß das System zum Speichern und Aufbewahren von Patientendaten, einschließlich schriftlicher und graphischer Unterlagen, beim Inhaber ausgelegt ist. Dafür kann das System geeignete Eingabemedien, wie einen Scanner enthalten.

Vorzugsweise enthält der erste Teil der Speichereinrichtungen einen Notfalldatenspeicherbereich, in dem Verwaltungsdaten und die Daten eines Notfallausweises, eines Organspendeausweises, Notfalltestaments u.ä. des Inhabers speicherbar sind. Ein Zugriff auf diese Daten sollte durch die Berechtigungsprüfeinrichtungen frei oder mit nur einer Arzt- oder Rettungsdienstkennung, die vorzugsweise über eine spezielle Arzt- oder Rettungsdienstkarte oder eine Arzt-/Rettungsdienst-Zugriffsgerätekennung in die Berechtigungsprüfeinrichtungen eingebbar ist, oder mit nur einer Inhaberkennung freigebbar sein.

Weiterhin ist es bevorzugt, daß der erste Teil der Speichereinrichtungen einen Übersichtsdatenspeicherbereich enthält, in dem eine Auflistung wichtiger anamnestischer Daten, einschließlich einer ggf. erfolgten Verabreichung von Blut oder Blutprodukten und eine Dokumentation wichtiger Gesundheits-/Krankheitsdaten, einschließlich Allergie-, Impf-, Röntgen-, Schrittmacher-, Diabetiker-, Medikamentendaten u.ä., analog einer ärztlichen Patientenkarte gespeichert werden kann. Zusätzlich zu den vorstehenden im Zusammenhang mit den Notfalldaten angegebenen Zugriffsberechtigungen kann hier noch ein Zugriff durch Krankenkassen mittels einer entsprechenden Kennung vorgesehen sein.

Alle diese Zugriffsrechte können ferner für einen im ersten Teil der Speichereinrichtungen enthaltenen Behandlungsdatenspeicherbereich, in dem ein vorgegebener zeitlicher Rahmen und eine vorgegebene inhaltliche Struktur von Vorsorgeuntersuchungen sowie Untersuchungen im Rahmen der Nachsorge chronischer und/oder bösartiger Erkrankungen speicherbar sind, und für einen optionalen oder zusätzlichen Nachweisdatenspeicherbereich eingestellt sein, der im ersten Teil der Speichereinrichtungen enthalten ist und in dem zumindest eine vorgebbare Anzahl und/oder Art von Zugriffen auf die Speichereinrichtungen insbesondere einschließlich der jeweils erfolgten vorzugsweise individuellen Berechtigungs- und/oder Authentizitätserkennung und vorgenommenen Zugriffsart im einzelnen speicherbar ist.

Eine vorzugsweise Gestaltung des ersten Teils der Speichereinrichtungen kann einen Dokumentationsbereich enthalten, in dem die im Laufe des Lebens des Inhabers der Speichereinrichtungen anfallenden relevanten Gesundheits-/Krankheitsdaten einschließlich Anamnese, Diagnosen, Befunde wie Labor-, Blutdruckwerte, etc. speicherbar sind.

Eine vorzugsweise Gestaltung des zweiten Teils der Speichereinrichtungen kann einen Dokumentationsbereich enthalten, in dem alle Originalunterlagen von Arztberichten, Zeugnissen, Röntgen-, Ultraschall-, Computertomographie-, Endoskopieabbildungen

usw., Biosignale, wie EKG- und EEG-Daten etc., direkt oder als Graphiken u.ä. speicherbar sind.

Ein Zugriff auf die vorgenannten Dokumentationsbereiche ist zumindest soweit durch die Berechtigungsprüfeinrichtungen einzeln oder in Kombination mit einer Arztkennung, welche vorzugsweise über eine spezielle Arztkarte oder eine Arzt-Zugriffsgerätekennung in die Berechtigungsprüfeinrichtungen eingebbar ist, mit einer Inhaberkennung und/oder einer Krankenkassenkennung freigebbar.

Auch der zweite Teil der Speichereinrichtungen kann bei einer bevorzugten Ausgestaltung einen Nachweisdatenspeicherbereich enthalten, der grundsätzlich genauso funktioniert, wie der Nachweisdatenspeicherbereich im ersten Teil der Speichereinrichtungen. Eine vorteilhafte Weiterbildung davon besteht darin, daß der Nachweisdatenspeicherbereich im ersten Teil der Speichereinrichtungen schieberegisterartig aufgebaut ist, so daß sein ältester Inhalt zur insbesondere endgültigen Abspeicherung in den Nachweisdatenspeicherbereich des zweiten Teils der Speichereinrichtungen zur Platzschaffung für einen Neueintrag im Nachweisdatenspeicherbereich im ersten Teil der Speichereinrichtungen Platz verschiebbar ist. Damit können die Nachweisdaten jederzeit gespeichert werden. Es kann insbesondere auch bei anderen Einsatzgebieten des persönlichen Archivierungssystems nach der Erfindung vorgesehen werden, daß nur die letzten etwa drei bis fünf Zugriffsinformationen gespeichert bleiben und ältere Zugriffsinformationen gelöscht werden.

Vorteilhafterweise kann eine bereits bestehende und bei der Bevölkerung eingeführte Karte, wie eine Krankenversicherungskarte, ein Personalausweis oder eine Kontokarte, die Speichereinrichtungen des erfindungsgemäßen Personendaten-Archivierungssystems ganz oder teilweise aufnehmen.

Für eine weitere Erhöhung der Sicherheit der archivierten Daten ist es bevorzugt, daß mittels den Berechtigungsprüfeinrichtungen ein insbesondere turnusmäßiger Kennungswechsel einer Anwender- und/oder Gerätekennung zur Berechtigungs- und/oder

Authentizitätserkennung berücksichtigt werden kann. Dabei wird vorzugsweise mittels den Berechtigungsprüfeinrichtungen eine Authentizitäts- und/oder Berechtigungsprüfung von Anwender, Zugriffsgeräten und/oder Speichereinrichtungen für einen beabsichtigten Zugriff durchgeführt.

Die Verwendungsmöglichkeit der Daten im Personendaten-Archivierungssystem nach der Erfindung wird weiter dadurch optimiert, daß die Speichereinrichtungen eine Mehrzahl von Bereichen enthalten, denen unterschiedliche Zugriffssicherungen, wie Passwörter, PINs o.ä. zugeordnet werden können.

Ein besonderer weiterer Schutz kann bei der Erfindung vorteilhaft für Schreibzugriffe vorgesehen sein, indem Speicherungen von neuen oder geänderten Daten auf die Speichereinrichtungen dort nur nach Eingabe einer Signatur zusammen mit dieser abspeicherbar sind, und daß letztere vorzugsweise durch eine Anwender- und/oder Zugriffsgerätekennung insbesondere automatisch erzeugt wird.

Nachfolgend werden einige weitere bevorzugte Ausführungsformen angegeben, die sich aus verschiedenen Merkmalskombinationen der Unteransprüche ergeben.

Beispielsweise als Patientenkarte kann eine Prozessor-Chipkarte Verwendung finden, die sowohl zumindest einen Teil der Berechtigungsprüfeinrichtungen in Form des Prozessors als auch einen ersten Teil der Speichereinrichtungen auf dem Chip enthält, um ein Patientendaten-Archivierungssystem zu realisieren. Mit einer derartigen Prozessor-Chipkarte kann der Informationsaustausch im Medizinbereich verbessert werden. In erster Linie dient die Prozessor-Chipkarte dabei als Kontroll- und Sicherheitselement, und die Speicherfunktion ist insbesondere auf Grund der üblicherweise geringen Speicherkapazität solcher Karten zweitrangig. Das erfindungsgemäße System enthält daher neben der Karte einen mobilen eigentlichen Datenspeicher, wofür sich beispielsweise eine magneto-optische Platte in Form einer 2,5-Zoll-Diskette eignet. Diese Datenträger sind so klein und handlich wie eine Chipkarte, verfügen aber über eine Speicherkapazität von beispielsweise 140 Megabyte und sind wiederbeschreibbar.

Die durch die Erfindung geschaffene Sicherheit wird technologisch durch die Kombination der Prozessor-Chipkarte mit einem bezüglich dieser externen Massendatenspeicher erreicht. Der Zugriff zu dem Massendatenspeicher erfolgt ausschließlich über die Prozessor-Chipkarte mit ihren Sicherheitseinrichtungen zur Berechtigungsprüfung und Zugriffsfreigabe. Damit sind die Daten z.B. auf der magneto-optischen Platte in gleicher Weise geschützt, als ob sie auf der Prozessor-Chipkarte selbst abgelegt wären.

Somit hat ein Patient in dieser Zeit der zunehmenden medizinischen Aufsplittung mehr als nur einen medizinischen Ausweis und wird in die Lage versetzt, seine relevanten Krankheitsdaten selbst komplett zu dokumentieren, um sie dann beispielsweise dem jeweils behandelnden Arzt oder seiner Versicherung zur Verfügung stellen zu können. Die durch die Erfindung somit allgemein mögliche umfassende persönliche und insbesondere medizinische Datensammlung in der Hand des Patienten trägt zu einer Verbesserung des Informationsaustausches z.B. zwischen den Ärzten bei. Gleichzeitig ist sie, um beim Beispiel des Patientendaten-Archivierungssystems zu bleiben, ein Instrument zur Qualitätssicherung der ärztlichen Leistung und dient einer ganzheitlichen Betreuung des Patienten. Die Vermeidung von Datenverlusten z.B. bei einem Arztwechsel führt zu einer Reduzierung der erforderlichen Untersuchungen und damit zu einer Entlastung, gesundheitsmäßig beim Patienten und kostenmäßig bei den Krankenkassen.

Eine Datensammlung über die Krankengeschichte darf sich aber nicht in einer Auflistung von anamnestischen Daten, Diagnosen oder durchgeführten Untersuchungen erschöpfen. Jeder weiterbehandelnde Arzt möchte zumindest die kompletten Arzt- und Krankenhausberichte einsehen, und häufig will er verständlicherweise auch nicht darauf verzichten, die Originalaufzeichnungen und -befunde betrachten zu können. Eine solche umfassende Datensammlung wäre aber auf einer herkömmlichen Prozessor-Chipkarte alleine nicht realisierbar, sondern nur in Kombination mit einem typischen Datenspeicher, für den es ohne die Erfindung keinen ausreichenden Datenschutz gäbe.

In Fortführung des vorbeschriebenen Ausführungsbeispiels kann die Prozessor-Chipkarte zunächst als Notfall-Ausweis fungieren. Neben den typischen Notfalldaten kann der entsprechende Speicherteil bei Interesse auch als zum Speichern eines Organspendeausweises oder Notfalltestaments eingesetzt werden. Mögliche Zugriffsregelungen hierfür wurden bereits weiter oben beschrieben. Durch die Mitwirkung des Inhabers über einen Zugriffsschlüssel, wie ein Passwort oder eine PIN wird daraus eine umfassende Ausweiskarte mit den wesentlichen medizinischen (oder bei anderen Anwendungsfällen Finanz-, Versicherungs-, "Kleingeldguthaben-") Basisdaten. Zusammen mit dem z.B. elektronischen Massenspeichermedium für die Komplettdaten erhält der Patient eine vollständige Sammlung von wichtigen Krankheitsdaten, wobei die Arztberichte, Bilder (beispielsweise Röntgen- und Ultraschallbilder) und Biosignale (EKG u.a.) im Original vorliegen. Aus praktischen Überlegungen kann die Mitwirkung des Patienten bei der Zugriffsfreigabe für einen Arzt, der sich z.B. neben seinem Kartenlesegerät und seinem Laufwerk für die Berechtigungsprüfeinrichtungen beispielsweise mit einer Arztkarte identifiziert hat, darauf beschränkt werden, daß auf der Prozessor-Chipkarte ein Foto des Patienten den Karteninhaber ausweist.

Es kann ferner eine automatisch arbeitende Einrichtung vorgesehen sein, die dafür sorgt, daß der Speicher einer gefüllten Prozessor-Chipkarte durch Auslagern von Daten auf z.B. eine zugehörige MO-Platte wieder zum Aufnehmen weiterer neuer Daten bereit ist.

Weiterhin ist bei der Ausführung mit der Prozessor-Chipkarte als Kontroll- und Sicherheitsinstrument eine Ausstattung mit einem Coprozessor möglich, durch den für das Sicherheitskonzept eine Authentifikation von Terminal, Karte und Benutzer sowie eine Dokumentation über jeden Zugriff auf die abgelegten Daten erfolgen kann.

Als Berechtigungsprüfeinrichtungen und deren Prüfmittel sind insbesondere Prozessoreinrichtungen vorzugsweise auf einem Teil der oder allgemein den Speichereinrichtungen und/oder aber in einem Steuerrechner oder Zugriffsgerät und geeignete Programme bzw. Zugriffsgeräte-, Speichereinrichtungs-, Inhaber- und Anwenderkennun-

gen zu nennen. Die Sicherung kann beispielsweise ferner auch oder zusätzlich dadurch erreicht werden, daß die Kennungen getrennter Speichervorrichtungen und insbesondere Datenträger kombiniert werden müssen, um auf geschützte Daten zugreifen zu können. Ferner können die Daten direkt in lauffähigen Programmdateien enthalten sein, deren Aufruf von bestimmten Kennungen abhängt. Der erfindungsgemäße Grundschutz wird aber dadurch erreicht, daß ein Zugriff vom Prüfergebnis der Berechtigungsprüfeinrichtungen abhängt.

Das erfindungsgemäße System kann zwar z.B. eine Arztkartei schon wegen der bestehenden Dokumentationspflicht nicht ersetzen. Die Erfindung schafft aber eine wichtige Ergänzungsmöglichkeit beispielsweise zur Arztkartei, da durch das Patientendaten-Archivierungssystem sämtliche relevanten Daten vollständig, unverfälscht und unmittelbar zur Verfügung stehen. Für die digitale Archivierung spricht ferner, daß zahlreiche Daten bereits jetzt, zumindest aber künftig, von vornherein in digitaler Form vorliegen, wie Röntgenbilder, Ultraschallaufnahmen, EKG, EEG, Arzberichte usw.

Weitere vorteilhafte und bevorzugte Ausgestaltungen der Erfindung ergeben sich durch die Ansprüche und deren Kombinationen.

Nachfolgend werden Einzelheiten der Erfindung unter Bezugnahme auf die Zeichnungen näher angegeben, in denen:

Figur 1 eine schematische Darstellung von Systemkomponenten eines Personendaten-Archivierungssystems zeigt,

Figuren 2a - 2c tabellarische Darstellungen möglicher Aufteilungen der Speichereinrichtungen sind, und

Figur 3 ein Blockschaltbild des Aufbaus von Figur 1 ist.

In den Figuren 1 und 3 ist ein Personendaten-Archivierungssystem 1 gezeigt. Das System 1 enthält transportable oder mobile, persönliche Speichereinrichtungen 2 zum Speichern und Aufbewahren von Personendaten beim Inhaber. Die Speichereinrichtungen enthalten erste und zweite getrennte Datenträger 8 und 9, die einzelne Speichervorrichtungen als ersten und zweiten Teil 6 bzw. 7 der Speichereinrichtungen 2 bilden.

Zum Zugreifen auf die einzelnen Datenträger 8, 9 ist ein Zugriffsgerät 12 gezeigt, das ein kombiniertes Lesegerät und Laufwerk für die beiden Datenträger 8, 9 darstellt. Ferner ist das Zugriffsgerät 12 auch ausgelegt, eine Berechtigungskarte 13 zu lesen.

Der erste Datenträger 6 ist eine Prozessor-Chipkarte und dient sowohl zur Speicherung kleinerer Datenmengen, beispielsweise eines Notfallausweises, von Übersichtsdaten und/oder Behandlungsdaten des Inhabers und von Nachweisdaten erfolgter Speicherzugriffe, als auch als Bestandteil von Berechtigungsprüfeinrichtungen 3, wofür die Prozessoreinrichtungen 10 der Karte eingesetzt werden. Wie insbesondere der Figur 3 deutlich zu entnehmen ist, sind im Zugriffsgerät 12 weitere Prozessoreinrichtungen 10 vorgesehen, die ebenfalls Bestandteil der Berechtigungsprüfeinrichtungen 3 zur Feststellung einer Zugriffsberechtigung sind.

Der zweite Datenträger 7 ist eine magneto-optische Platte und ermöglicht so eine Speicherung großer Datenmengen zur Speicherung von Detaildaten. Außerdem ist durch die Prozessoreinrichtungen 10 eine Steuerung vorgesehen, um zu vermeiden, daß die Prozessor-Chipkarte speichermäßig voll ist und keine weiteren Daten mehr aufnehmen kann, wofür Daten von der Prozessor-Chipkarte immer wieder auf die magneto-optische Platte ausgelagert werden.

Die den Speichereinrichtungen 2 zugeordneten Berechtigungsprüfeinrichtungen 3 dienen der Datensicherheit, da sie dafür sorgen, daß nur in Abhängigkeit von einer positiven Berechtigungs- und/oder Authentizitätserkennung ein Zugriff auf zumindest einige der auf den persönlichen Speichereinrichtungen 2 gespeicherten Personendaten frei-

gegeben werden kann. Bei dem gezeigten Ausführungsbeispiel sind hierfür die einzelnen Prozessoreinrichtungen 10 und später noch genauer angegebene Kennungen zuständig.

Die Berechtigungsprüfeinrichtungen 3 des gezeigten Ausführungsbeispiels sind so ausgeführt, daß sie einen turnusmäßiger Kennungswechsel einer Anwender- und/oder Gerätekennung zur Berechtigungs- und/oder Authentizitätserkennung berücksichtigen und eine Authentizitäts- und/oder Berechtigungsprüfung von Anwender, Zugriffsgeräten und Speichereinrichtungen 2 für einen beabsichtigten Zugriff durchführen. Weiterhin können Schreibzugriffe auf die Speichereinrichtungen 2 dort nur nach Eingabe einer Signatur zusammen mit dieser abgespeichert werden, wobei diese Signatur durch eine Anwender- bzw. Zugriffsgerätekennung automatisch unter Nutzung des RSA-Verfahrens erzeugt wird.

Das gezeigte Archivierungssystem 1 ist so ausgelegt, daß nur in Verbindung mit dem ersten Teil 6 der Speichereinrichtungen 2 auf den zweiten Teil 7 der Speichereinrichtungen 2 zugegriffen werden kann. Es sind auch mehrere verschiedene Prüf- bzw. Berechtigungsstufen vorgesehen, um den Zugriff auf verschiedene Datenbereiche zu regeln.

In einer ersten Prüfstufe wird nur eine Lesegerätekennung überprüft, um einen Zugriff auf Notfalldaten zuzulassen. In dieser oder einer höheren Prüfstufe kann eventuell eine Berechtigungskarte für den Zugriff auf Daten erforderlich sein, die eine Übersicht über weitere persönliche Daten des Inhabers der Chipkarte geben. Eine weitere Prüfstufe kann dadurch realisiert werden, daß auf die auf dem zweiten Teil 7 der persönlichen Speichereinrichtungen 2 gespeicherten Personendaten, wie Detaildaten, nur in Abhängigkeit von einer positiven Berechtigungs- und/oder Authentizitätserkennung mittels der Berechtigungsprüfeinrichtungen 3 zugreifbar ist. Eine solche Kennung kann z.B. folgende Informationen alleine oder kombiniert berücksichtigen: eine Lesegerätekennung, eine Laufwerkskennung, eine Datenträgerkennung, eine Anwenderkennung, eine Inhaberkennung. Insbesondere die beiden letzteren können auch durch PINs

(persönliche Identifizierungsnummern) oder Geheimzahlen o.ä. realisiert werden, wobei verschiedene Eingaben zu unterschiedlichen Berechtigungsstufen führen können. Die einzelnen Prüfstufen der Berechtigungsprüfeinrichtungen 3 können beispielsweise auch dafür genutzt werden, um für Schreib- und Lesezugriffe jeweils unterschiedliche Berechtigungen zu vergeben.

Im Zusammenhang mit dem Kartenlesegerät wird durch die Berechtigungsprüfeinrichtungen 3 die Authentizität der Prozessor-Chipkarte überprüft. Dabei können z.B. gefälschte Karten abgewiesen werden. Ebenso wird anhand der Prozessor-Chipkarte mittels der Berechtigungsprüfeinrichtungen 3 eine Überprüfung des Kartenlesegeräts durchgeführt, so daß nicht autorisierte Lesegeräte überhaupt keinen Zugriff auf die Daten der Prozessor-Chipkarte und auch des Massenspeichers erhalten. Eine ähnliche gegenseitige Autorisierungsüberprüfung kann auch für die magneto-optische Platte und das entsprechende Laufwerk vorgesehen sein.

Im einzelnen werden die Identifikationsmerkmale des Kartenlesegeräts (z.B. Unikat-Nr.) und des Laufwerks für die magneto-optische Platte erfaßt (z.B. Laufwerkkennung) erfaßt und die entsprechenden Daten auf oder in dem Speicher der Prozessor-Chipkarte gespeichert, sobald das Lesegerät oder das Laufwerk auf gespeicherte Daten zugreift. Sollte die Kapazität des entsprechenden Speichers auf der Prozessor-Chipkarte nicht ausreichen, werden ältere Daten auf die MO-Platte ausgelagert oder gelöscht. Durch eine Erfassung der Benutzeridentifikation (Anwender- und Inhaberkennungen) wird getrennt für die Prozessor-Chipkarte und die MO-Platte jeglicher Zugriff auf die gespeicherten Daten erfaßt. Alternativ oder auch ergänzend zu anderen Identifikationsmerkmalen, wie der Lesegerätekennung oder einer Benutzerkennung, kann eine Berechtigungskarte zur Autorisierungsprüfung benötigte Daten bereitstellen, die den Benutzer ausweisen und ebenfalls gespeichert werden können, um dort, wo verschiedene Benutzer auf das gleiche Kartenlesegerät zugreifen, wie z.B. in einem Rettungswagen, eine einfache, schnelle und sichere Berechtigungserkennung zu ermöglichen.

Die umfangreichen Daten auf dem zweiten Teil 7 der Speichereinrichtungen 2, also beispielsweise Bilddaten auf der MO-Platte, können nur dann gelesen werden, wenn ein Benutzer beispielsweise über entsprechende Programmteile verfügt, was aber erst nach positiver Authentizitätsprüfung möglich ist.

Als weiteren Sicherheitsaspekt enthält das Zugriffsgerät 12 in dem gezeigten Beispiel Kryptoeinrichtungen 11, die für eine Entschlüsselung und Verschlüsselung bei Lese- bzw. Schreibzugriffen auf die Teile 6 und 7 der Speichereinrichtungen 2 sorgen und beispielsweise zur Bearbeitung von großen Datenmengen zumindest einen als Coprozessor ausgelegten Kryptoprozessor enthalten. Die Kryptoeinrichtungen 11 sind den Speichereinrichtungen 2 vorgeschaltet und werden betriebsmäßig mittels der Berechtigungsprüfeinrichtungen 3 zur Bearbeitung von Zugriffen auf die Speichereinrichtungen 2 freigegeben. Die zwischen einzelnen Speichervorrichtungen bzw. deren Zugriffseinrichtungen 12 und den Rechnereinrichtungen 14 transferierten Daten werden durch die Kryptoeinheit ent- bzw. verschlüsselt, wobei letztere ebenfalls erst nach positiv ausgefallener Authentizitätsprüfung in Funktion tritt. Beim Aufruf einer Datei auf der MO-Platte wird diese automatisch entschlüsselt. Umgekehrt erfolgt eine automatische Verschlüsselung einer Datei, wenn sie auf die MO-Platte geschrieben wird. Die entsprechenden Dateinamen sind beim System 1 ohne die Freigabe durch die Berechtigungsprüfeinrichtungen 3 nicht lesbar und auf der Prozessor-Chipkarte hinterlegt. Die hohe Datentransferrate kann durch die eigenständige Kryptoeinheit bewältigt werden.

Der erste Teil der Speichereinrichtungen 2 bzw. die erste Speichervorrichtung 6 ist nicht auf die vorbeschriebenen Ausführung beschränkt, sondern kann eine magnetische, magneto-optische oder optische Speicherfläche oder ein Speicherchip insbesondere auf oder in einer vorzugsweise etwa scheckkartengroßen Kunststoffkarte als Datenträger 8 sein. Ebenfalls ist die Ausgestaltung des zweiten Teils der Speichereinrichtungen 2 bzw. der zweiten Speichervorrichtung 7 nicht auf eine magneto-optische Platte beschränkt, sondern kann jeglicher elektronische, magnetische, magneto-optische oder optische Massenspeicher insbesondere in Form einer 2,5 oder 3,5 Zoll großen Diskette oder einer PCMCIA-Einheit als Datenträger 9 sein.

Die Speichereinrichtungen 2 sind jeweils durch ein zum Hinzufügen und/oder Ändern von Personendaten wiederbeschreibbares Speichermedium 4, 5 entsprechend den Datenträgern 8, 9 gebildet. Für bestimmte Anwendungszwecke sind wenigstens Teile der beiden beschreibbaren Speichermedien 4, 5 schreibgeschützt oder schreibschützbar. Hierdurch können beispielsweise unveränderliche Eintragungen vor versehentlichen Überschreibungen geschützt werden. Auch Bereiche des Speichermediums 5 des zweiten Datenträgers können aus dem gleichen Grund schreibgeschützt oder schreibschützbar sein, um z.B. nachträgliche Änderungen in der Zugriffsdokumentation auszuschließen.

Die Prozessoreinrichtungen 10 erfüllen neben ihrer Aufgabe zur Berechtigungsüberprüfung noch die Steuerung von zumindest Teilen der Speichereinrichtungen 2 und/oder die wenigstens teilweise Steuerung von Zugriffen auf letztere.

Nicht gesondert gezeigt sind Kopierschutzeinrichtungen, Druckausgabeschutzeinrichtungen und Ausgabebeschränkungseinrichtungen, die ein unerwünschtes Kopieren, Drucken oder andersartiges Ausgeben von den Speichereinrichtungen 2 entnommenen Daten verhindern, wenn diese entsprechenden Einrichtungen nicht durch einen geeigneten Berechtigungsnachweis den Berechtigungsprüfeinrichtungen gegenüber neutralisiert, d.h. abgeschaltet sind.

Statt des oder zusätzlich zum gezeigten Zugriffsgerät 12 können für die einzelnen Datenträger 8 und 9 sowie die Berechtigungskarte 13 gesonderte Zugriffsgeräte vorgesehen sein, beispielsweise persönliche, mobile und/oder stationäre Zugriffsgeräte. Das Zugriffsgerät 12 ist sowohl für die Prozessor-Chipkarte als auch die magneto-optische Platte in Minidisk-Form für einen Schreib- und/oder Lesezugriff ausgelegt.

Jedes einsetzbare Zugriffsgerät 12 enthält zweckmäßigerweise entsprechend den Formaten von die Speichereinrichtungen 2 aufnehmenden Datenträgern Kartenlesegeräte für z.B. Magnetstreifen- oder Chipkarten, Diskettenlaufwerke für z.B. magnetische,

magneto-optische oder optische Disketten, CD-ROM-Laufwerke und/oder Aufnahmen für PCMCIA-Einheiten. Auch bei getrennter Ausführung der Zugriffsgeräte 12 für die ersten und zweiten Teile 6, 7 der Speichereinrichtungen 2 können diese Geräte 12 zusammengeschaltet und über diese Zusammenschaltung von den Berechtigungsprüfeinrichtungen 3 ein entsprechender Berechtigungsnachweis erfaßt werden.

Zur Erstellung von Sicherungskopien, die bei Verlust der Speichereinrichtungen 2 einen vollständigen Datenverlust verhindern, lassen die Zugriffsgeräte 12 direkt oder die Berechtigungsprüfeinrichtungen 3 ohne Berechtigungsnachweis eine Erstellung von Sicherungskopien der transportablen, persönlichen Speichereinrichtungen 2 zu. Hierfür können z.B. flüchtige Speichereinrichtungen in dem entsprechenden Zugriffsgerät 12 enthalten sein, um Daten zum Kopieren zwischenzuspeichern.

Wie den Figuren 1 und 3 weiter zu entnehmen ist, ist zum Ansteuern des Zugriffsgeräts 12 eine Rechnereinrichtung 14 in Form eines PCs vorgesehen. Diese Rechnereinrichtungen 14 dienen ferner als Anzeige- und Ein-/Ausgabegeräte von Daten sowohl für die Berechtigungsprüfeinrichtungen 3 als auch die Speichereinrichtungen 2, um Daten zu suchen, auszugeben und einzugeben.

Das in der Figur 1 dargestellte Zugriffsgerät 12 ist über eine Leitung mit einer nicht näher bezeichneten eigenen Tastatur und über eine weitere Leitung an geeigneten Datenschnittstellen mit den Rechnereinrichtungen 14 verbunden. Die Rechnertastatur und/oder die Zugriffsgerätetastatur kann zum Eingeben von PINs u.ä. verwendet werden können. Ferner ist das Zugriffsgerät 12 mit nicht näher bezeichneten Displayeinrichtungen versehen.

Der erste Datenträger 8 ist gleichzeitig eine Krankenversicherungskarte und das gesamte System 1 dient zur Archivierung von Patientendaten einschließlich schriftlicher und graphischer Unterlagen beim Inhaber. Jedoch können auch andere Daten mit diesem oder ähnlichen Systemen archiviert werden, wie beispielsweise Finanzdaten, Versicherungsdaten, Reisedaten u.v.m.

Für den Anwendungsfall des Patientendaten-Archivierungssystems ist in den Figuren 2a - 2c tabellarisch eine Speicherorganisation dargestellt. Die Figur 2a zeigt die Organisationsstruktur der beiden Datenträger, die Figur 2b gibt Aufschluß über den Inhalt der enthaltenen Notfallkarte und die Figur 2c erläutert den Inhalt der patientenkarte, wobei die verschiedenen Speicherbereiche direkt bezeichnet sind, so daß keine weiteren Erläuterungen zu ihrem Verständnis erforderlich sind. In der Praxis können einzelne Felder und Einträge über die Rechnereinrichtungen 14 mittels Menü- oder Fenstertechnik aufgerufen werden.

Wenn vorstehend auf ein Patientendaten-Archivierungssystem, Patientendaten und allgemein den Medizinbereich Bezug genommen wurde, so ist dies nur exemplarisch zu verstehen. Die Erfindung betrifft ein Personendaten-Archivierungssystem, das durch die in den Ansprüchen angegebenen Merkmale und Merkmalskombinationen bestimmt und nicht auf einzelne Ausführungsbeispiele der Beschreibung beschränkt ist. So können z.B. mehr als zwei (separate) Speichereinrichtungsteile vorgesehen sein, wobei beispielsweise eine einzige Prozessorkarte mit mehreren MO-Platten für je ein eigenes Sachgebiet zusammenarbeiten kann. Insbesondere sind alle durch die Merkmalsformulierungen in den Ansprüchen enthaltenen Ausführungsmöglichkeiten der Erfindung ohne Einschränkungen und mit den dem Fachmann geläufigen Modifikationen und Substitutionen im Umfang der Erfindung abgedeckt.

Bezugszeichenliste

1	Personendaten-Archivierungssystem
2	Speichereinrichtungen
3	Berechtigungsprüfeinrichtungen
4, 5	Speichermedium
6	erster Teil der Speichereinrichtungen
7	zweiter Teil der Speichereinrichtungen
8, 9	erste und zweite Datenträger
10	Prozessoreinrichtungen
11	Kryptoeinrichtungen
12	Zugriffsgeräte
13	Berechtigungskarte, Arzt- oder Rettungsdienstkarte
14	Rechnereinrichtungen

Ansprüche

1. Personendaten-Archivierungssystem mit transportablen, persönlichen Speichereinrichtungen zum Speichern und Aufbewahren von Personendaten beim Inhaber,

dadurch gekennzeichnet,

daß den Speichereinrichtungen (2) Berechtigungsprüfeinrichtungen (3) zugeordnet sind, mittels denen nur in Abhängigkeit von einer positiven Berechtigungs- und/oder Authentizitätserkennung ein Zugriff auf zumindest einige der auf den persönlichen Speichereinrichtungen (2) gespeicherten Personendaten freigebbar ist.

2. Personendaten-Archivierungssystem nach Anspruch 1,

dadurch gekennzeichnet,

daß mittels den Berechtigungsprüfeinrichtungen (3) eine Mehrzahl von Prüfstufen ausführbar ist.

3. Personendaten-Archivierungssystem nach Anspruch 1 oder 2,

dadurch gekennzeichnet,

daß zumindest ein Teil der Speichereinrichtungen (2) durch ein zum Hinzufügen und/oder Ändern von Personendaten beschreibbares und insbesondere wiederbeschreibbares Speichermedium (4, 5) gebildet ist.

4. Personendaten-Archivierungssystem nach Anspruch 3,

dadurch gekennzeichnet,

daß die Berechtigungsprüfeinrichtungen (3) zum Freigeben eines Lese- und/oder Schreibzugriffs auf das beschreibbare Speichermedium (4, 5) in Abhängigkeit von einer insbesondere entsprechenden Berechtigungs- und/oder Authentizitätserkennung ggf. in einer zugehörigen Prüfstufe ausgelegt sind.

5. Personendaten-Archivierungssystem nach Anspruch 3 oder 4,

dadurch gekennzeichnet,

daß zumindest ein Teil des beschreibbaren Speichermediums (4, 5) schreibgeschützt oder schreibschützbar ist.

6. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß die Speichereinrichtungen (2) einen ersten Teil (6) und zumindest einen zweiten Teil (7) mit insbesondere unterschiedlichen Speicherkapazitäten enthalten.

7. Personendaten-Archivierungssystem nach Anspruch 6,

dadurch gekennzeichnet,

daß der erste, insbesondere kapazitätsmäßig kleinste Teil (6) der Speichereinrichtungen (2) ein Ausweis-, Identifikations- oder Stammdatenspeicherteil ist.

8. Personendaten-Archivierungssystem nach Anspruch 6 oder 7,

dadurch gekennzeichnet,

daß auf die auf dem ersten Teil (6) der persönlichen Speichereinrichtungen (2) gespeicherten Personendaten, wie Ausweis-, Identifikations- oder Stammdaten, unabhängig von den Berechtigungsprüfeinrichtungen (3) oder mit einer positiven Berechtigungs- und/oder Authentizitätserkennung in einer ersten Prüfstufe der Berechtigungsprüfeinrichtungen (3) zugreifbar ist.

9. Personendaten-Archivierungssystem nach einem der Ansprüche 6 bis 8,

dadurch gekennzeichnet,

daß nur in Verbindung mit wenigstens dem ersten Teil (6) der Speichereinrichtungen (2) auf den zumindest einen zweiten Teil (7) der Speichereinrichtungen (2) zugreifbar ist.

10. Personendaten-Archivierungssystem nach einem der Ansprüche 6 bis 9,

dadurch gekennzeichnet,

daß der zweite, relativ zum ersten Teil (6) kapazitätsmäßig größere Teil (7) der Speichereinrichtungen (2) ein Detaildatenspeicherteil ist.

11. Personendaten-Archivierungssystem nach einem der Ansprüche 6 bis 10,
dadurch gekennzeichnet,
daß auf die auf dem zweiten Teil (7) der persönlichen Speichereinrichtungen (2) gespeicherten Personendaten, wie Detaildaten, nur in Abhängigkeit von einer positiven Berechtigungs- und/oder Authentizitätserkennung ggf. in einer zweiten Prüfstufe mittels der Berechtigungsprüfeinrichtungen (3) zugreifbar ist.

12. Personendaten-Archivierungssystem nach einem der Ansprüche 6 bis 11,
dadurch gekennzeichnet,
daß die wenigstens ersten und zweiten Teile der Speichereinrichtungen (2) durch separate erste bzw. zweite Speichervorrichtungen (6, 7) insbesondere auf verschiedenen ersten bzw. zweiten Datenträgern (8, 9) gebildet sind.

13. Personendaten-Archivierungssystem nach einem der Ansprüche 6 bis 12,
dadurch gekennzeichnet,
daß der erste Teil der Speichereinrichtungen (2) bzw. die erste Speichervorrichtung (6) eine magnetische, magneto-optische oder optische Speicherfläche oder ein Speicherchip insbesondere auf oder in einer vorzugsweise etwa scheckkartengroßen Kunststoffkarte als Datenträger (8) ist.

14. Personendaten-Archivierungssystem nach einem der Ansprüche 6 bis 13,
dadurch gekennzeichnet,
daß der zweite Teil der Speichereinrichtungen (2) bzw. die zweite Speichervorrichtung (7) ein elektronischer, magnetischer, magneto-optischer oder optischer Massenspeicher insbesondere in Form einer 2,5 oder 3,5 Zoll großen Diskette oder einer PCMCIA-Einheit als Datenträger (9) ist.

15. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß zumindest einem Teil der Speichereinrichtungen (2) zugeordnete und/oder vorzugsweise wenigstens einen Teil der Berechtigungsprüfeinrichtungen (3) bildende Prozessoreinrichtungen (10) vorgesehen sind, die vorzugsweise auf dem Datenträger (8), wie z.B. einer Kunststoffkarte, angeordnet sind und insbesondere einen Prozessor enthalten.

16. Personendaten-Archivierungssystem nach den Ansprüchen 13 und 15,

dadurch gekennzeichnet,

daß die Prozessoreinrichtungen (10) zur Steuerung von zumindest Teilen der Speichereinrichtungen (2) und/oder zur wenigstens teilweisen Steuerung von Zugriffen auf letztere und/oder zumindest als Teil der Berechtigungsprüfeinrichtungen (3) ausgelegt sind.

17. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß den Speichereinrichtungen (2) Kryptoeinrichtungen (11) vorgeschaltet sind, deren Betrieb insbesondere mittels der Berechtigungsprüfeinrichtungen (3) zur Bearbeitung von Zugriffen auf die Speichereinrichtungen (2) freigebbar ist.

18. Personendaten-Archivierungssystem nach Anspruch 15 oder 16 und Anspruch 17,

dadurch gekennzeichnet,

daß die Kryptoeinrichtungen (11) in den Prozessoreinrichtungen (10) enthalten sind und vorzugsweise einen Kryptoprozessor aufweisen.

19. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß Kopierschutzeinrichtungen vorgesehen sind, mittels denen ein Speichern von zumindest einigen Daten, die auf den persönlichen Speichereinrichtungen (2), insbesondere ggf. deren zweiten Teil (7), gespeichert sind, auf bezüglich letzteren externen Speichern unterbindbar ist und/oder ein Speichern von zumindest einigen Daten, die auf dem ersten Teil (6) der Speichereinrichtungen (2) gespeichert sind, auf bezüglich letzteren externen Speichern zulaßbar sind.

20. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß Druckausgabeschutzeinrichtungen vorgesehen sind, mittels denen eine Druckausgabe von zumindest einigen Daten unterbindbar ist, die auf den persönlichen Speichereinrichtungen (2), insbesondere ggf. deren zweiten Teil (7), gespeichert sind und/oder ein Drucken von zumindest einigen Daten zulaßbar ist, die auf dem ersten Teil (6) der Speichereinrichtungen (2) gespeichert sind.

21. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß Ausgabebeschränkungseinrichtungen vorgesehen sind, mittels denen eine Ausgabe von zumindest einigen Daten, die auf den persönlichen Speichereinrichtungen (2), insbesondere ggf. deren zweiten Teil (7), gespeichert sind, auf mehr als ein Ausgabemedium z.B. eines Rechners, wie zusätzliche Bildschirme des Rechners oder eine Netzwerkkarte des Rechners zur Verbindung mit weiteren extern angeordneten Rechnern, unterbindbar ist.

22. Personendaten-Archivierungssystem nach einem der Ansprüche 19 bis 21,

dadurch gekennzeichnet,

daß die Kopierschutzeinrichtungen, Druckausgabeschutzeinrichtungen und/oder Ausgabebeschränkungseinrichtungen mittels der Berechtigungsprüfeinrichtun-

gen (3) durch eine entsprechende positive Berechtigungs- und/oder Authentizitätserkennung ggf. in einer zugehörigen Prüfstufe neutralisierbar sind.

23. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß die Berechtigungsprüfeinrichtungen (3) ausgelegt sind, Gerätekennungen von Zugriffsgeräten (12) für die Handhabung der Speichereinrichtungen (2) in eine Prüfung zur Berechtigungs- und/oder Authentizitätserkennung ggf. zur Erfüllung einer insbesondere ersten Prüfstufe einzubeziehen.

24. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß die persönlichen Speichereinrichtungen (2) Kennungen aufweisen, die von den Berechtigungsprüfeinrichtungen (3) in eine Prüfung zur Berechtigungs- und/oder Authentizitätserkennung ggf. zur Erfüllung einer insbesondere ersten Prüfstufe einbeziehbar sind.

25. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß die Berechtigungsprüfeinrichtungen (3) ausgelegt sind, Benutzer- und/oder Inhaberidentifikationen von zumindest einem Anwender bzw. dem Inhaber, dessen Daten in den Speichereinrichtungen (2) archiviert sind, in eine Prüfung zur Berechtigungs- und/oder Authentizitätserkennung ggf. zur Erfüllung einer insbesondere zweiten Prüfstufe und ggf. weiterer Prüfstufen zur Freigabe eines Zugriffs auf zumindest einige der auf den persönlichen Speichereinrichtungen (2) gespeicherten Personendaten einzubeziehen.

26. Personendaten-Archivierungssystem nach Anspruch 25,

dadurch gekennzeichnet,

daß die Berechtigungsprüfeinrichtungen (3) ausgelegt sind, eine Anwenderkennung, wie eine Benutzer- bzw. Inhaberidentifikation über manuelle und/oder elektronische Eingaben, wie beispielsweise von einer Berechtigungskarte (13), durchzuführen.

27. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß durch die Berechtigungsprüfeinrichtungen (3) zugelassene Zugriffe auf den Speichereinrichtungen (2) mit den dafür relevanten Daten, wie Gerätekennungen von Zugriffsgeräten (12) und/oder Benutzer- und/oder Inhaberidentifikationen, insbesondere auf den Speichereinrichtungen (2) selbst dokumentierbar sind.

28. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß persönliche Zugriffsgeräte (12) vorgesehen sind, mittels denen vom Inhaber, dessen Daten in den Speichereinrichtungen (2) archiviert sind, und/oder von Anwendern der Speichereinrichtungen (2) in Abhängigkeit von einer insbesondere entsprechenden Berechtigungs- und/oder Authentizitätserkennung ggf. in einer zugehörigen Prüfstufe auf zumindest einige der archivierten Daten zum Zweck der Information, Datenänderung/-ergänzung und/oder Weitergabe auch über Datenfernübertragung zugreifbar ist.

29. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß mobile und/oder stationäre Zugriffsgeräte (12) vorgesehen sind, mittels denen von Anwendern in Abhängigkeit von einer insbesondere entsprechenden Berechtigungs- und/oder Authentizitätserkennung ggf. in einer zugehörigen

Prüfstufe auf zumindest einige der archivierten Daten zum Zweck der Information und/oder Datenänderung/-ergänzung zugreifbar ist.

30. Personendaten-Archivierungssystem nach Anspruch 28 oder 29,
dadurch gekennzeichnet,
daß die Zugriffsgeräte (12) für einen Schreib- und/oder Lesezugriff zumindest auf einige der auf den persönlichen Speichereinrichtungen (2) gespeicherten Personendaten in Abhängigkeit von einer insbesondere entsprechenden Berechtigungs- und/oder Authentizitätserkennung ggf. in einer zugehörigen Prüfstufe ausgelegt sind.

31. Personendaten-Archivierungssystem nach einem der Ansprüche 28 bis 30,
dadurch gekennzeichnet,
daß die Zugriffsgeräte (12) Gerätekennungen aufweisen, die von den Berechtigungsprüfeinrichtungen (3) zur Prüfung einer Berechtigungs- und/oder Authentizitätserkennung ggf. zur Erfüllung einer insbesondere ersten Prüfstufe erfaßbar sind, und daß die Gerätekennung vorzugsweise durch eine in zumindest ein Zugriffsgerät (12) eingebbare Anwenderkennung aktivierbar ist.

32. Personendaten-Archivierungssystem nach einem der Ansprüche 28 bis 31,
dadurch gekennzeichnet,
daß zum Ansteuern der Zugriffsgeräte (12) herkömmliche Rechnereinrichtungen (14) vorgesehen sind.

33. Personendaten-Archivierungssystem nach einem der Ansprüche 28 bis 32,
dadurch gekennzeichnet,
daß die Zugriffsgeräte (12) entsprechend den Formaten von die Speichereinrichtungen (2) aufnehmenden Datenträgern Kartenlesegeräte für z.B. Magnetstreifen- oder Chipkarten, Diskettenlaufwerke für z.B. magnetische, magnetooptische oder optische Disketten, CD-ROM-Laufwerke und/oder Aufnahmen für PCMCIA-Einheiten enthalten.

34. Personendaten-Archivierungssystem nach einem der Ansprüche 28 bis 33,

dadurch gekennzeichnet,

daß zumindest zwei Zugriffsgeräte (12) zur Zusammenschaltung von entsprechenden Datenträgern (8, 9) der Speichereinrichtungen (2) kombiniert sind und diese Zusammenschaltung von den Berechtigungsprüfeinrichtungen (3) zum Berechtigungsnachweis oder ggf. als eine erste Prüfstufe erfaßbar ist.

35. Personendaten-Archivierungssystem nach einem der Ansprüche 28 bis 34,

dadurch gekennzeichnet,

daß die Zugriffsgeräte (12) ausgelegt sind, ohne Berechtigungsnachweis oder ggf. in einer ersten Prüfstufe Sicherungskopien der transportablen, persönlichen Speichereinrichtungen (2) zu erstellen.

36. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß herkömmliche Rechnereinrichtungen (14) als Anzeige- und Ein-/Ausgabegeräte von Daten vorgesehen sind.

37. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß es zum Speichern und Aufbewahren von Patientendaten, einschließlich schriftlicher und graphischer Unterlagen, beim Inhaber ausgelegt ist.

38. Personendaten-Archivierungssystem nach den Ansprüchen 6 und 37,

dadurch gekennzeichnet,

daß der erste Teil (6) der Speichereinrichtungen (2) einen Notfalldatenspeicherbereich enthält, in dem Verwaltungsdaten und die Daten eines Notfallausweises, eines Organspendeausweises, Notfalltestaments u.ä. des Inhabers speicherbar

sind und auf den ein Zugriff zumindest soweit durch die Berechtigungsprüfeinrichtungen (3) frei oder mit nur einer Arzt- oder Rettungsdienstkennung, die vorzugsweise über eine spezielle Arzt- oder Rettungsdienstkarte (13) oder eine Arzt-/Rettungsdienst-Zugriffsgerätekennung in die Berechtigungsprüfeinrichtungen (3) eingebbar ist, oder mit nur einer Inhaberkennung freigebbar ist.

39. Personendaten-Archivierungssystem nach den Ansprüchen 6 und 37 oder Anspruch 38,

dadurch gekennzeichnet,

daß der erste Teil (6) der Speichereinrichtungen (2) einen Übersichtsdatenspeicherbereich enthält, in dem eine Auflistung wichtiger anamnestischer Daten, einschließlich einer ggf. erfolgten Verabreichung von Blut oder Blutprodukten und eine Dokumentation wichtiger Gesundheits-/Krankheitsdaten, einschließlich Allergie-, Impf-, Röntgen-, Schrittmacher-, Diabetiker-, Medikamentendaten u.ä., analog einer ärztlichen Patientenkarte speicherbar sind und auf den ein Zugriff zumindest soweit durch die Berechtigungsprüfeinrichtungen (3) frei oder einzeln oder in Kombination mit einer Arzt- oder Rettungsdienstkennung, die vorzugsweise über eine spezielle Arzt- oder Rettungsdienstkarte (13) oder eine Arzt-/Rettungsdienst-Zugriffsgerätekennung in die Berechtigungsprüfeinrichtungen (3) eingebbar ist, mit einer Inhaberkennung und/oder einer Krankenkassenkennung freigebbar ist.

40. Personendaten-Archivierungssystem nach den Ansprüchen 6 und 37 oder Anspruch 38 oder 39,

dadurch gekennzeichnet,

daß der erste Teil (6) der Speichereinrichtungen (2) einen Behandlungsdatenspeicherbereich enthält, in dem ein vorgegebener zeitlicher Rahmen und eine vorgegebene inhaltliche Struktur von Vorsorgeuntersuchungen sowie Untersuchungen im Rahmen der Nachsorge chronischer und/oder bösartiger Erkrankungen speicherbar sind und auf den ein Zugriff zumindest soweit durch die Berechtigungsprüfeinrichtungen (3) einzeln oder in Kombination mit einer Arztkennung,

die vorzugsweise über eine spezielle Arztkarte (13) oder eine Arzt-Zugriffsgerätekennung in die Berechtigungsprüfeinrichtungen (3) eingebbar ist, mit einer Inhaberkennung und/oder einer Krankenkassenkennung freigebbar ist.

41. Personendaten-Archivierungssystem nach den Ansprüchen 6 und 37 oder einem der Ansprüche 38 bis 40,

dadurch gekennzeichnet,

daß der erste Teil (6) der Speichereinrichtungen (2) einen Nachweisdatenspeicherbereich enthält, in dem zumindest eine vorgebbare Anzahl und/oder Art von Zugriffen auf die Speichereinrichtungen (2) insbesondere einschließlich der jeweils erfolgten vorzugsweise individuellen Berechtigungs- und/oder Authentizitätserkennung und vorgenommenen Zugriffsart im einzelnen speicherbar ist und auf den ein Zugriff zumindest soweit durch die Berechtigungsprüfeinrichtungen (3) einzeln oder in Kombination mit einer Arztkennung, die vorzugsweise über eine spezielle Arztkarte (13) oder eine Arzt-Zugriffsgerätekennung in die Berechtigungsprüfeinrichtungen (3) eingebbar ist, mit einer Inhaberkennung und/oder einer Krankenkassenkennung freigebbar ist.

42. Personendaten-Archivierungssystem nach den Ansprüchen 6 und 37 oder einem der Ansprüche 38 bis 41,

dadurch gekennzeichnet,

daß der zweite Teil (7) der Speichereinrichtungen (2) einen Dokumentationsbereich enthält, in dem alle Originalunterlagen von Arztberichten, Zeugnissen, Röntgen-, Ultraschall-, Computertomographieabbildungen usw., Biosignale, wie EKG- und EEG-Daten etc., direkt oder als Graphiken u.ä. speicherbar sind und auf den ein Zugriff zumindest soweit durch die Berechtigungsprüfeinrichtungen (3) einzeln oder in Kombination mit einer Arztkennung, die vorzugsweise über eine spezielle Arztkarte (13) oder eine Arzt-Zugriffsgerätekennung in die Berechtigungsprüfeinrichtungen (3) eingebbar ist, mit einer Inhaberkennung und/oder einer Krankenkassenkennung freigebbar ist.

43. Personendaten-Archivierungssystem nach den Ansprüchen 6 und 37 oder einem der Ansprüche 38 bis 42,

dadurch gekennzeichnet,

daß der zweite Teil (7) der Speichereinrichtungen (2) einen Nachweisdatenspeicherbereich enthält, in dem zumindest eine vorgebbare Anzahl und/oder Art von Zugriffen oder alle Zugriffe auf die Speichereinrichtungen (2) insbesondere einschließlich der jeweils erfolgten vorzugsweise individuellen Berechtigungs- und/oder Authentizitätserkennung und vorgenommenen Zugriffsart im einzelnen speicherbar ist und auf den ein Zugriff zumindest soweit durch die Berechtigungsprüfeinrichtungen (3) einzeln oder in Kombination mit einer Arztkennung, die vorzugsweise über eine spezielle Arztkarte (13) oder eine Arzt-Zugriffsgerätekennung in die Berechtigungsprüfeinrichtungen (3) eingebbar ist, mit einer Inhaberkennung und/oder einer Krankenkassenkennung freigebbar ist.

44. Personendaten-Archivierungssystem nach den Ansprüchen 41 und 43,

dadurch gekennzeichnet,

daß der Nachweisdatenspeicherbereich im ersten Teil (6) der Speichereinrichtungen (2) schieberegisterartig aufgebaut ist, so daß sein ältester Inhalt zur insbesondere endgültigen Abspeicherung in den Nachweisdatenspeicherbereich des zweiten Teils (7) der Speichereinrichtungen (2) zur Platzschaffung für einen Neueintrag im Nachweisdatenspeicherbereich im ersten Teil (6) der Speichereinrichtungen (2) Platz verschiebbar ist.

45. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß die Speichereinrichtungen (2) ganz oder teilweise Bestandteil einer Krankenversicherungskarte, eines Personalausweises oder einer Kontokarte sind.

46. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß mittels den Berechtigungsprüfeinrichtungen (3) ein insbesondere turnusmäßiger Kennungswechsel einer Anwender- und/oder Gerätekennung zur Berechtigungs- und/oder Authentizitätserkennung berücksichtigbar ist.

47. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß mittels den Berechtigungsprüfeinrichtungen (3) eine Authentizitäts- und/oder Berechtigungsprüfung von Anwender, Zugriffsgeräten (12) und/oder Speichereinrichtungen (2) für einen beabsichtigten Zugriff durchführbar ist.

48. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

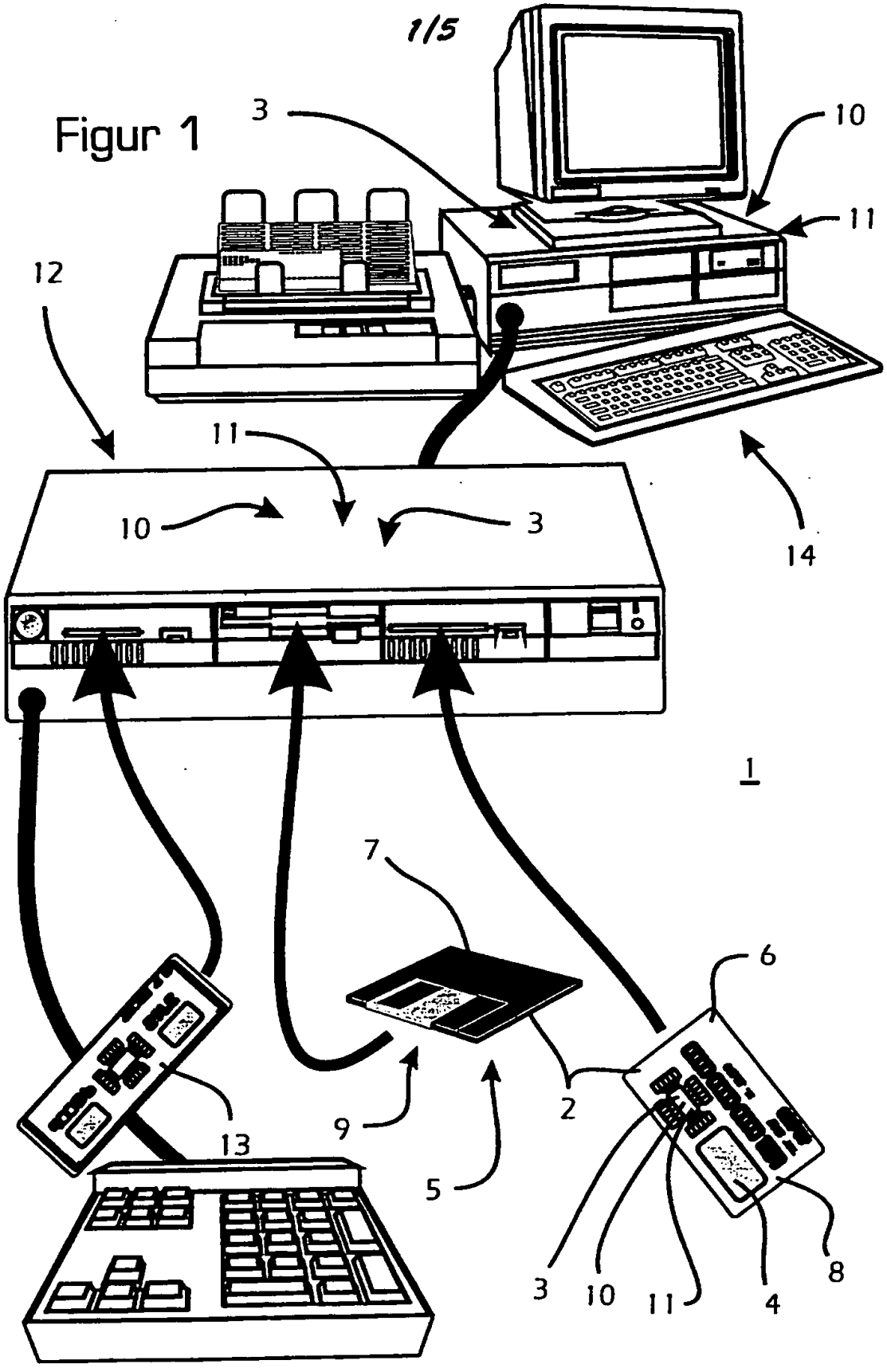
daß die Speichereinrichtungen (2) eine Mehrzahl von Bereichen enthalten, denen unterschiedliche Zugriffssicherungen, wie Passwörter, PINs, Berechtigungskarten (13) o.ä. zuordenbar sind.

49. Personendaten-Archivierungssystem nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet,

daß Schreibzugriffe auf die Speichereinrichtungen (2) dort nur nach Eingabe einer Signatur zusammen mit dieser abspeicherbar sind, und daß letztere vorzugsweise durch eine Anwender- und/oder Zugriffsgerätekennung insbesondere automatisch erzeugbar ist.

Figur 1



- **Prozessor-Chipkarte**
- **Notfallkarte:**
  - Persönliche Angaben
  - Im Notfall zu verständigen
  - Behandelnde Ärzte
  - Unbedingt beachten
  - Blutgruppe
  - Organspendeausweis
  - Patiententestament
- **Patientenkarte:**
  - Anamnese-Datensatz
  - Diagnostik-Datensatz
  - Labor-Datensatz
  - Ausweise
  - Dauerdiagnosen
  - Dauermedikation
  - Vorsorge-Datensatz
  - Nachsorgedatensatz
  - Datensatz für Gesundheitsprogramme

- **Datenspeicher**
  - Texte
  - Bilder
  - Biosignale
  - Labordaten
  - Dokumentation und Planung von Vorsorgeuntersuchungen, Nachsorge von chronischen Krankheiten oder Tumorleiden
  - Gesundheitsprogramme
  - Software

Figur 2a

Prozessor-Chipkarte

Notfallkarte

Angaben zur Person:

Name, Vorname, Geburtsdatum, Postleitzahl, Wohnort, Straße, Telefon (Keine Angaben zur Krankenversicherung, KV-Nr. o.ä.)

Im Notfall verständigen:

Name, Vorname, Postleitzahl, Wohnort, Straße, Telefon (Hinweis auf ggf. zusätzliche und alternative Personen)

Behandelnde Ärzte:

Name, Vorname, Praxisadresse: Postleitzahl, Wohnort, Straße, Telefon, Fachrichtung (Hinweis auf ggf. zusätzliche Ärzte)

Unbedingt beachten:

Für die Notfallversorgung wichtige Erkrankungen oder Anomalien, z.B. Unverträglichkeit bzw. Allergie auf Medikamente (Medikamentenname, internationale Kurzbezeichnung der Wirksubstanz, Art der Reaktion), erschwerte Intubation, Narkosezwischenfälle, Cerebrales Krampfleiden, Diabetes mellitus, Marcumartherapie, Niereninsuffizienz, Dialysebehandlung, Glaukom, Kontaktlinsen, künstliches Auge, Herzschrittmacher, Situs inversus, Cholinesterasemangel, Porphyrie, Haemophilie, Sonstiges

Blutgruppe, Rhesusfaktor:

Blutgruppe (A, B, 0), Rhesusfaktor Rh-pos (D+)/Rh-neg (D-)), Antikörper

Organspendeausweis:

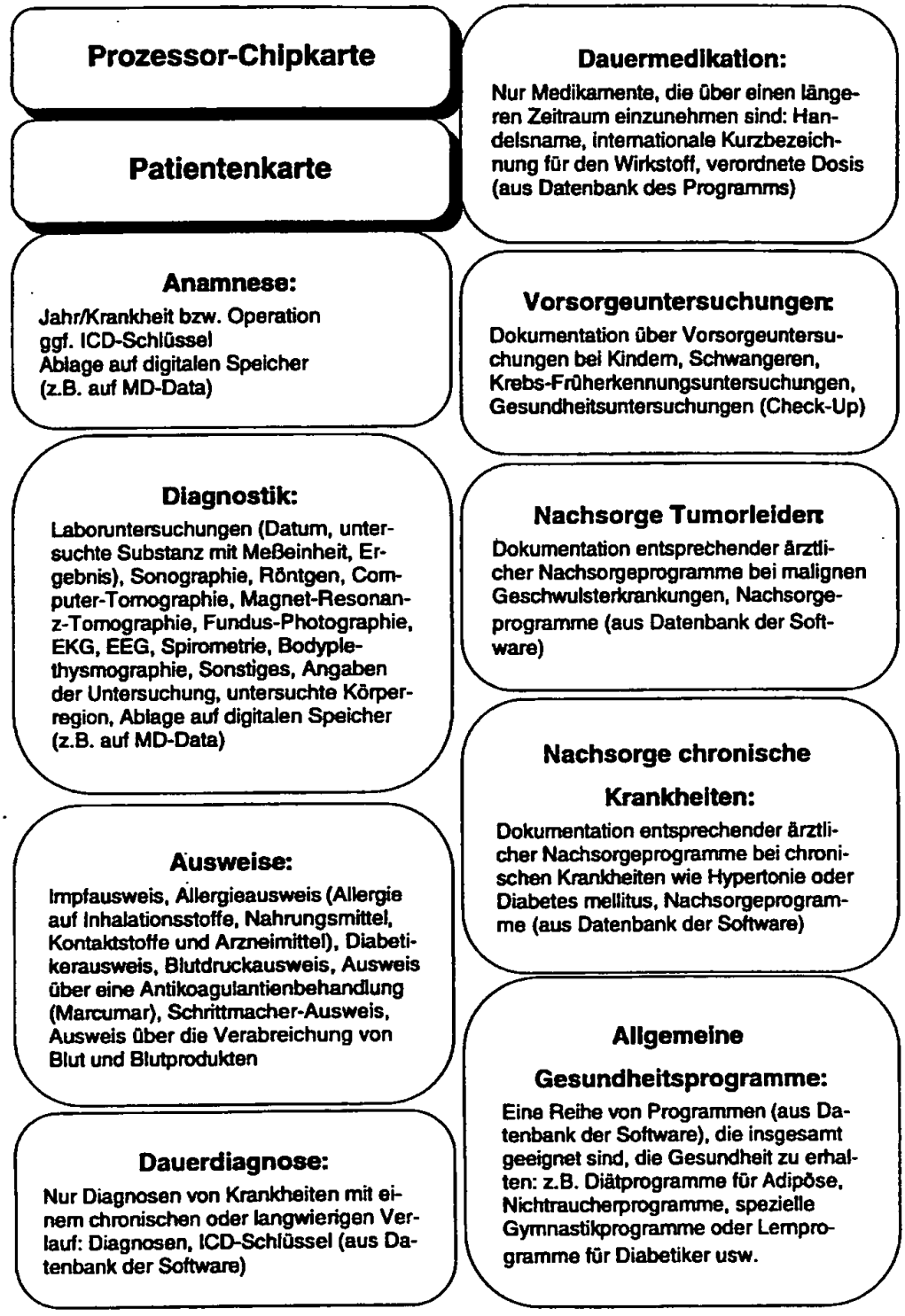
Ich bin Organspender für Transplantationen: ja/nein
Im Falle meines Todes bitte Nachricht geben an: Adresse, Telefon

Patiententestament:

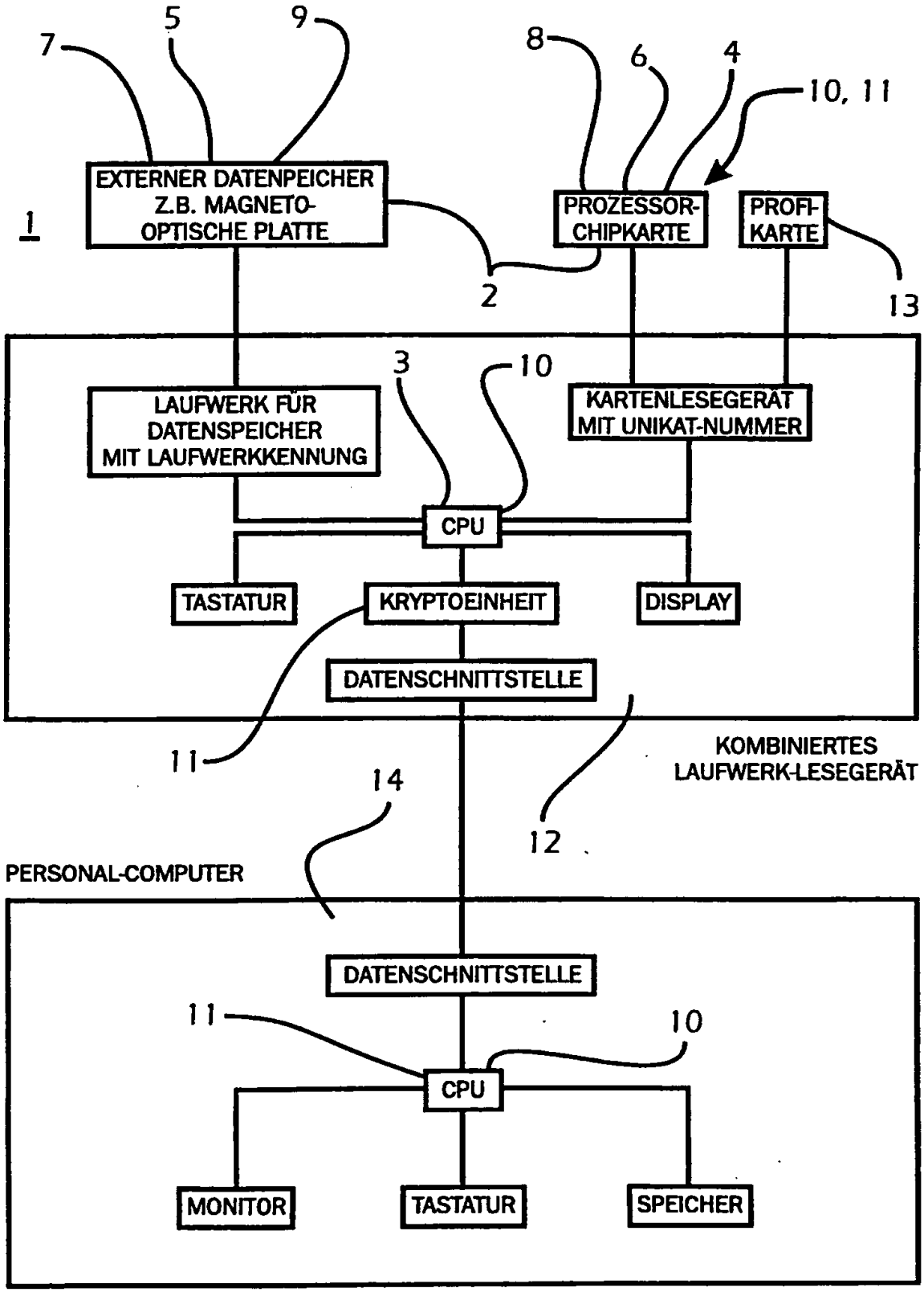
Ich bestimme für den Falle einer schweren Erkrankung oder eines schweren Unfalls als Ausdruck meines Willens für meine Familie und meine Ärzte folgendes:
Künstliche Lebensverlängerung:
Ich verfüge hiermit, daß mein Leben ...
Ort, Datum, Signatur
Betreuungsverfügung:
Folgende Personen sind berechtigt, von den behandelnden Ärzten detaillierte Auskünfte über meinen Gesundheitszustand sowie über diagnostische und therapeutische Maßnamen einzuholen. Für diesen Personenkreis entbinde ich die behandelnden Ärzte ausdrücklich von ihrer Schweigepflicht:
Name, Adresse, Telefon
Ich ermächtige für den Fall, daß ich nicht ansprechbar oder nicht zurechnungsfähig bin, folgende Personen für mich im Sinne des Betreuungsgesetzes und im Einklang mit meinem Patiententestament zu handeln und die Einwilligung zu medizinisch notwendigen Maßnamen und Eingriffen zu geben oder zu verweigern: Name, Adresse, Telefon

Ort, Datum, Unterschrift

Figur 2b


Prozessor-Chipkarte
Patientenkarte
Anamnese:
Jahr/Krankheit bzw. Operation
ggf. ICD-Schlüssel
Ablage auf digitalen Speicher
(z.B. auf MD-Data)
Diagnostik:
Laboruntersuchungen (Datum, untersuchte Substanz mit Meßeinheit, Ergebnis), Sonographie, Röntgen, Computer-Tomographie, Magnet-Resonanz-Tomographie, Fundus-Photographie, EKG, EEG, Spirometrie, Bodyplethysmographie, Sonstiges, Angaben der Untersuchung, untersuchte Körperregion, Ablage auf digitalen Speicher (z.B. auf MD-Data)
Ausweise:
Impfausweis, Allergieausweis (Allergie auf Inhalationsstoffe, Nahrungsmittel, Kontaktstoffe und Arzneimittel), Diabetikerausweis, Blutdruckausweis, Ausweis über eine Antikoagulantienbehandlung (Marcumar), Schrittmacher-Ausweis, Ausweis über die Verabreichung von Blut und Blutprodukten
Dauerdiagnose:
Nur Diagnosen von Krankheiten mit einem chronischen oder langwierigen Verlauf: Diagnosen, ICD-Schlüssel (aus Datenbank der Software)
Dauermedikation:
Nur Medikamente, die über einen längeren Zeitraum einzunehmen sind: Handelsname, internationale Kurzbezeichnung für den Wirkstoff, verordnete Dosis (aus Datenbank des Programms)
Vorsorgeuntersuchungen:
Dokumentation über Vorsorgeuntersuchungen bei Kindern, Schwangeren, Krebs-Früherkennungsuntersuchungen, Gesundheitsuntersuchungen (Check-Up)
Nachsorge Tumorleiden:
Dokumentation entsprechender ärztlicher Nachsorgeprogramme bei malignen Geschwulsterkrankungen, Nachsorgeprogramme (aus Datenbank der Software)
Nachsorge chronische Krankheiten:
Dokumentation entsprechender ärztlicher Nachsorgeprogramme bei chronischen Krankheiten wie Hypertonie oder Diabetes mellitus, Nachsorgeprogramme (aus Datenbank der Software)
Allgemeine Gesundheitsprogramme:
Eine Reihe von Programmen (aus Datenbank der Software), die insgesamt geeignet sind, die Gesundheit zu erhalten: z.B. Diätprogramme für Adipöse, Nichtraucherprogramme, spezielle Gymnastikprogramme oder Lernprogramme für Diabetiker usw.

Figur 2c


7
5
9
8
6
4
10, 11
EXTERNER DATENPEICHER Z.B. MAGNETO-OPTISCHE PLATTE
1
PROZESSOR-CHIPKARTE
PROFI-KARTE
2
13
3
10
LAUFWERK FÜR DATENSPEICHER MIT LAUFWERKKENNUNG
KARTENLESEGERÄT MIT UNIKAT-NUMMER
CPU
TASTATUR
KRYPTOEINHEIT
DISPLAY
DATENSCHNITTSTELLE
11
KOMBINIERTES LAUFWERK-LESEGERÄT
14
12
PERSONAL-COMPUTER
DATENSCHNITTSTELLE
11
10
CPU
MONITOR
TASTATUR
SPEICHER

Figur 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 95/03597

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00 G06F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO,A,90 12464 (LANG GERALD S) 18 October 1990 see page 7, line 4 - page 10, line 1; figure 1 ---	1-16
A	FR,A,2 680 258 (BALLET ERIC ;BALLET GERARD (FR)) 12 February 1993 see abstract; claims 1,5 --- -/--	1-16, 25-30, 32-34, 36,38, 45,48

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 January 1996	01.02.96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Fournier, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 95/03597

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	COMPUTERS & SECURITY, JUNE 1985, NETHERLANDS, vol. 4, no. 2, ISSN 0167-4048, pages 123-134, HIGHLAND H J 'Microcomputer security: data protection techniques' see page 126, column 2, line 9 - page 127, column 2, line 21 ---	1-20
A	DE,A,42 13 797 (BAVARIA MEDIZIN TECHNOLOGIE GM) 28 October 1993 see page 1, column 1, line 1 - page 3, column 1, line 56; claim 1 -----	1

1

INTERNATIONAL SEARCH REPORT

..nformation on patent family members

Inter. ..onal Application No
PCT/EP 95/03597

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A-9012464	18-10-90	CA-A-	1329657	17-05-94
		EP-A-	0465571	15-01-92
		US-A-	5065429	12-11-91
		US-A-	5191611	02-03-93
FR-A-2680258	12-02-93	WO-A-	9303457	18-02-93
DE-A-4213797	28-10-93	NONE		

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 95/03597

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06F1/00 G06F19/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO,A,90 12464 (LANG GERALD S) 18.Oktober 1990 siehe Seite 7, Zeile 4 - Seite 10, Zeile 1; Abbildung 1 ---	1-16
A	FR,A,2 680 258 (BALLET ERIC ;BALLET GERARD (FR)) 12.Februar 1993 siehe Zusammenfassung; Ansprüche 1,5 --- -/--	1-16, 25-30, 32-34, 36,38, 45,48

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
17.Januar 1996	01. 02. 96

Name und Postanschrift der Internationale Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Fournier, C

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 95/03597

C(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	COMPUTERS & SECURITY, JUNE 1985, NETHERLANDS, Bd. 4, Nr. 2, ISSN 0167-4048, Seiten 123-134, HIGHLAND H J 'Microcomputer security: data protection techniques' siehe Seite 126, Spalte 2, Zeile 9 - Seite 127, Spalte 2, Zeile 21	1-20
A	DE,A,42 13 797 (BAVARIA MEDIZIN TECHNOLOGIE GM) 28.Oktober 1993 siehe Seite 1, Spalte 1, Zeile 1 - Seite 3, Spalte 1, Zeile 56; Anspruch 1	1

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 95/03597

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO-A-9012464	18-10-90	CA-A-	1329657	17-05-94
		EP-A-	0465571	15-01-92
		US-A-	5065429	12-11-91
		US-A-	5191611	02-03-93
FR-A-2680258	12-02-93	WO-A-	9303457	18-02-93
DE-A-4213797	28-10-93	KEINE		